Research on Safety Protection Control of Equipment Terminal Access based on Power Private Network

Wang Ou1, Li Wei1, Jin Chengming1, Zhang Wenjie1, Yang mingyu1*

1 State Grid Liaoning Electric Power Co. LTD Information & Telecommunication Branch Company, Shenyang Liaoning 110000, China
*Corresponding author’s e-mail: sg_eiconf@126.com

Abstract. In this paper, based on the application requirements of the power industry for the wireless private network, the networking and security protection technology of the power wireless private network are studied. Firstly, it analyzes the necessity of establishing the electric power wireless private network, and then gives the system architecture and technical system of the electric power wireless private network; studies the security risks and Countermeasures Faced by the TD-LTE wireless private network, and analyzes the technical applicability of the TD-LTE wireless private network in combination with the electric power wireless technology policy, so as to provide a reference for the construction of the electric power wireless communication network.

1. Introduction

As one of the fastest-growing communication technologies in the field of information communication, wireless communication has been widely used in the field of public mobile communication. At present, LTE (long term evolution), including TDD (time division duplex) and FDD (frequency division duplex), the fourth generation global general cellular mobile communication technology standard, has been widely used in China since December 2013. In particular, TD-LTE system has covered more than 340 cities and rural areas, and has been applied in the field of public mobile communication on a large scale [1].

Information and communication system is the foundation of smart grid networking, operation and management, which runs through all aspects of smart grid generation, transmission, transformation, distribution, power consumption and dispatching. Since the 1970s, the construction of electric power communication network based on information communication system has developed continuously and rapidly. In the 21st century, the wireless communication technology represented by 4gTD-LTE wireless communication technology is widely used in the fields of wireless government affairs network, railway train control network, urban operation monitoring network, production safety management network, emergency command network, public safety supervision network and urban Internet of things, which also provides technical support and beneficial reference for the construction and development of power wireless communication network Take [2]. At present, the networking and security protection of power wireless private network has become one of the important directions of the development of power communication system. However, there are some defects in wireless network, such as low reliability, low bandwidth, large delay, high service interruption rate, which make the planning and construction of power wireless communication network face many difficulties. Therefore, it is of great significance to study and adopt TD-LTE wireless communication technology in the power wireless special network to realize the real-time data transmission and distribution intelligence of power grid monitoring [3-4].
Therefore, the construction and security protection technology of TD-LTE wireless private network by combining the TD-LTE system technical system, security risk, security protection mechanism and related electric power standards and specifications are studied in this paper. By referring to the advanced TD-LTE wireless communication technology, a wireless private network suitable for the power industry is constructed to realize flexible, convenient, safe and reliable access to various power distribution terminals.

2. Analysis on the demand of power network construction

At present, all levels of electric power communication networks in various provinces and cities in China still adopt the cable communication technology dominated by optical fiber and carrier communication. GPRS / CDMA public network and corresponding narrow-band private network only play an auxiliary role, and there are problems such as poor security, low reliability, and low traffic capacity. At the same time, due to the continuous growth of the current power business, the existing wireless assisted communication mode can not carry the high broadband business types such as video, image, business interaction, emergency response, etc., and has poor scalability and low connection rate. Especially in the case of power grid disaster, it may lead to the phenomenon that instructions can not be transmitted down, data can not be uploaded due to the bandwidth limitation, which makes the dispatching paralyzed and can not be started and resumed in a long time. Therefore, the practical problems mentioned above put forward an urgent demand for the construction of broadband wireless private network.

Compared with 3G technology, TD-LTE 4G technology at this stage has lower system cost, higher system capacity, higher data rate and shorter delay. Wireless technology is located in the network layer of the three-tier architecture of the Internet of things (sensing layer, network layer, application layer). It has strong technical advantages in network security, reliability, scalability and so on. It has a wide application prospect for the power industry. The application of TD-LTE wireless broadband technology in the power grid industry can provide safe and reliable communication guarantee for customers and business needs, and serve various links such as power generation production, transmission scheduling, power sale service and power safety. The "optical fiber + wireless" hybrid networking deployment strategy adopted has the following advantages: 1) large business load; 2) meeting the high bandwidth business requirements such as voice and video monitoring scheduling; 3) realizing real-time interaction, location service and high-speed data transmission capacity; 4) better QoS support capacity; 5) high transmission reliability and disaster tolerance prevention mechanism.

3. Network structure and technical scheme of power private network

3.1. Network structure of Power Private Network

TD-LTE system consists of core network and access network. According to the different communication functions, the core network is divided into mobile management entity, service gateway, packet data network gateway, home contract server and other devices, mainly responsible for signaling control, data processing and transmission, mobility management of communication terminals, contract data management, etc. The access network provides the wireless link between the terminal and the core network, and is responsible for connecting the core network and the end user. The access network with flat structure composed of base station only reduces the network element level and the transmission delay of data, which can meet the requirement of low delay in power wireless private network. The basic architecture of the power wireless private network system based on TD-LTE is shown in Figure 1.

The communication terminal is connected with the power distribution service terminal through the Ethernet port and is responsible for sending the data from the service terminal to the base station after layer by layer processing through the air interface protocol, and submitting the data from the base station to the service terminal after receiving and processing to the service terminal. The communication terminal needs to insert a global user identification card (USIM), which stores the user's root key, signing data, user's number and other information.
In order to provide a good coverage area, TD-LTE power wireless special network base station usually installs the RF remote end unit to a high and open place, and installs the baseband processing unit to the interior of the machine room, and uses DC power supply to interconnect with MSTP equipment through Ethernet port for data return. The base station is responsible for controlling the data transmission of the communication terminal in the airport and allocating the communication channel resources to the terminal. The core network is responsible for user authentication, the management of the session between the terminal and the core network, and the management of terminal mobility. The terminal communicates with the base station through the Uu Interface, and the base station establishes the transmission link through the X2 interface. The base station is connected with the core network through the S1 interface of the transmission network. The core network is composed of multiple devices, among which relevant control signaling or data are transmitted through S11, S6a, S5 and other standard interfaces.

Base stations in different frequency bands need to consider the bandwidth requirements corresponding to different services at the same time in order to take into account all types of services. For example, in the distribution network automation service, the service flow is that each "three remote", "two remote" and "one remote" terminal is centralized to the distribution network automation center master station. Each 110kV substation has about 100-200 10kV node equipment, and the communication bandwidth demand of each node equipment is about 1-5kbit/s, so in this service, about 1Mbit/s communication bandwidth is provided for each substation within the coverage; in the measurement automation service, because this service is mainly responsible for the monitoring and management of load and distribution transformer, each 110kV substation is about 600-1000 There are metering automation nodes with a transmission period of 15min, so each node is allocated a bandwidth of about 3Mbit/s in this service. In the mobile broadband office business, employees can use intelligent terminals to access the network through the power wireless broadband special network to realize remote mobile office, which is especially suitable for outdoor inspection and maintenance, so each terminal is allocated with a bandwidth of about 1Mbit/s. Due to the large demand of service bandwidth, the terminal should be located near the base station as far as possible to meet the bandwidth demand with high-order modulation. In the substation video monitoring service, due to the real-time requirements of video transmission, at least 2Mbit/s bandwidth shall be allocated to each video monitoring terminal. Because the throughput of the base station with low-order modulation far from the base station is difficult to meet the demand of video bandwidth, the video terminal should also be located as close to the base station as possible.
3.2. Analysis of technical characteristics of electric power wireless private network

SC-FDMA is used in TD-LTE special network and OFDM is used in downlink. Its frequency band is mainly applied for lower carrier frequency band, such as 230MHz. Therefore, TD-LTE multi carrier technology pays more attention to spectrum utilization and system coverage, which can meet the bandwidth requirements of power wireless communication special network.

In terms of transmission bandwidth, the transmission bandwidth allocated by domestic TD-LTE public network shall be at least 20MHz. The bandwidth resource of wireless private network is relatively tight compared with public network. Generally, the provincial radio management department divides 5MHz or 10MHz frequency resource for an industry or department in a certain region by means of temporary authorization.

In TD-LTE system, MIMO multi antenna technology is used to realize parallel transmission of space channel and increase space transmission resources. In the pursuit of higher communication quality and reliability, MIMO multi antenna technology can effectively improve the communication quality and data transmission rate without increasing the transmission power and bandwidth, and ensure the high reliability of the power wireless private network.

Wireless private network is generally a single-mode network of LTE technology, which has certain particularity in coverage, data flow, terminals and other aspects. The base station of the electric power wireless special network is mainly covered by key areas, without large-scale seamless coverage; the electric power service terminal is mainly data service, with low mobility requirements, low single point service flow, and the data volume of the uplink service is larger than that of the downlink service [5]. Power TD-LTE wireless private network is generally connected with power service terminal by CPE terminal or embedded module.

4. Key technology of TD-LTE power wireless private network security risk prevention

Communication security is an important factor to restrict the power wireless private network. According to the requirements of regulations on safety protection of secondary power system and general scheme for safety protection of power system issued by the State Electricity Regulatory Commission, the information communication network of power system follows the policy of "safety zoning, network exclusive, horizontal isolation and vertical authentication". The security risk prevention technology involved in the TD-LTE power wireless private network with security as the first priority has become the focus of the business departments [6].

The security risks of TD-LTE power wireless private network mainly come from four aspects: communication terminal, air interface, base station and core network. Communication terminal risks mainly include illegal USIM card access and illegal terminal access; air interface risks refer to the interception and tampering of air radio signals; base station risks mainly include the deception of user access through pseudo base station to control user behavior; And the core network risks mainly include the theft of user information through access to network management.

In view of the above security risks, TD-LTE system adopts security protection mechanisms such as user identity security, two-way authentication, encryption and integrity protection to improve the security capability and reliability of the network:

1) User identity security: TD-LTE system adopts two mechanisms: temporary identity and encrypted permanent identity to protect user identity. Temporary identity refers to the use of a frequently updated and temporarily assigned identity in the air interface to replace the permanent identity, so as to significantly reduce the probability of permanent identity intercepted by the air interface. Encrypting permanent identity refers to encrypting the transmitted identity as much as possible in the air interface.

2) Two way authentication: in order to deal with security risks such as "illegal USIM card access", pseudo base station, etc., TD-LTE wireless network adopts two-way authentication mode. The implementation principle is to save a key related to user ID on both the terminal side and the core network side, and check the other Party's key when the communication terminal accesses the network to determine whether it is legal. Through the authentication of the network to the end user, the illegal
end user can be prevented from accessing the network. Here, using cryptography to solve various problems becomes the core of solving problems.

3) Encryption and integrity protection: in response to security risks such as "air interface data is intercepted and tampered", TD-LTE system introduces two layers of security mechanisms, i.e. wireless access (as) layer security and non-wireless access (NAS) layer security, to encrypt and protect the signaling or data transmitted between terminal and base station, terminal and core network respectively.

5. Conclusion
The safety protection control of equipment terminal access based on power private network is studied. First of all, the necessity of establishing the electric power wireless private network is analyzed, and the system architecture and technical system of the electric power wireless private network is gived; Also this paper the security risks and countermeasures faced by the TD-LTE wireless private network is studied. At present, there are still some problems in the wireless private network technology in the power industry, such as imperfect standards, inconsistent spectrum resources, and insufficient operation and maintenance power, which largely restrict the large-scale application of TD-LTE wireless private network technology. Therefore, the application of TD-LTE technology in the electric power industry should be steadily promoted by the strategy of "lease based, small-scale pilot".

References
[1] Huang Sheng. Demand analysis and technical scheme of intelligent distribution network communication service [J]. Power System Communication, 2010, 31 (6): 10-12.
[2] Liu Jian, Zhao Shuren, Zhang Xiaoqing. Progress and some suggestions of distribution automation in China [J]. Automation of Electric Power Systems, 2012, 36 (19): 6-10.
[3] Liu Jianming, Zhao Feng, Zhang Yuexia, et al. New generation broadband wireless mobile communication technology for smart grid [J]. Power System Communication, 2009, 30 (204): 1-3.
[4] Liu Jin, Wang Lizhu, Zhang Hui, et al. Research on power wireless private network based on FDD-LTE 230 [J]. Electric Engineering, 2015, 6 (2): 47-51.
[5] WANG Wen-ye, XU Yi, Khan-na M. A survey on the communication architectures in smart grid [J]. Computer Networks, 2011, 55 (15): 3604-3629.
[6] S Sesia, I Toufik, M Baker. The UMTS long term evolution: from theory to practice [M]. Posts and Telecom Press, 2012: 89-122.