EVALUATING THE RELIABILITY AND SECURITY OF POWER DISTRIBUTION WIRELESS NETWORK

Liming Chen, Xuzhu Dong, Zhengrong Wu, Zhiwen Liu
Electrical Power Research Institute of CSG, China
{chenlm2, dongxz, wuzr, liuzw2}@csg.cn

Baoren Chen
China Southern Power Grid (CSG), China
chenbr@csg.cn

ABSTRACT

Wireless network is embracing unprecedented popularity in power distribution communication due to its flexible and cost-efficient coverage for the massive number of sparsely distributed service terminals. This paper evaluates the reliability and security of power distribution wireless networks. Technical suitability suggestions from the perspective of reliability are obtained based on the mapping between communication performance and service requirements. Security challenges on the protection of radio link and wireless terminals are analysed and overcome by proposed random-noise-disturbed encryption method and joint authentication scheme. The evaluations provide suggestions for the application of wireless network carrying power distribution services, and ensure the reliable and secure operation of power distribution network.

INTRODUCTION

The conventional wired communication technologies such as optical fibers and power lines face the challenges of high capital and operational expenditure when deployed in power distribution[1,2]. Meanwhile, the complex and frequently varying structure of distribution network demands for communication ways with flexible and efficient coverage for the massive number of sparsely located distribution terminals. Wireless technology, as one promising solution to achieve the last-mile coverage, has been widely used in power distribution to complement the wired communications.

Currently, the wireless technologies utilized in distribution communication could be categorized as public and private, both of which share the advantages of flexible coverage, low deployment cost, etc., while demonstrating distinguishing characteristics concerning the bandwidth and latency performance, reliability and security protection. Regarding the application of wireless technologies in power distribution, two problems are in urgent need to be solved:

On one hand, a comprehensive investigation on the reliability of wireless technologies is needed. Reliability refers to the performance parameters including bandwidth, latency as well as congestion ratio and their effects on the correct operations of power services. It is the determining factor in the choice of wireless network, e.g., whether the wireless public network could satisfy the stringent latency and online ratio requirement of remote control services, which require nearly real-time correspondence.

On the other hand, there still exist several security challenges that affect the safe operation of wireless systems[3], especially in the radio link. To be specific, the universal subscriber identity module (USIM), in which essential security information is stored, is not well protected such that the radio link is not power private. Meanwhile, the communication terminals are not authorized to enjoy the exclusive use of radio links.

Towards this end, this paper develops an analytical framework to reveal how the network reliability parameters including the bandwidth, latency as well as online ratio match with correct operations of various power services such as remote control and sensing, thus determining the choice of wireless technologies. Meanwhile, the potential security risks of wireless networks are analysed and a security protection scheme is proposed. The scheme consists of a random-noise-disturbed USIM encryption algorithm as well as a joint authentication of the USIM and terminals, which aims at overcoming the security challenges from access domains and ensuring the safe operation of power distribution network.

The contribution of this paper is two-fold. On one hand, the comprehensive investigation on the reliability of wireless technologies provides a detailed mapping between network parameters and service requirements, thus facilitating the selection and cost-benefit analysis of wireless networks from service-oriented perspectives. On the other hand, the proposed security access protection scheme eliminates the risks of cracking essential information stored in USIM, thus making the radio link "Private", and admits only the authenticated terminals, thus making the use of radio link "Exclusive".

The rest of this paper is organized as follow: Section II introduces the network architecture and analyses the reliability requirements and security challenges. Section III investigates on the communication performance and service requirements, thus obtaining the conclusion of technical suitability. Section IV proposes a security protection scheme to enhance the safety operation of wireless network. Section V concludes the paper.

PROBLEM ANALYSIS

Currently, China Southern Power Grid (CSG) employs approximately two million public or private wireless communication terminals to transmit power distribution services, most of which are remote sensing and telemetry. A comprehensive study on the reliability and security of wireless network when carrying remote control and protection services is in urgent need to be conducted.

Architecture

The utilization of wireless network in CSG usually

deploys the architecture as illustrated in Fig.1, including both public and private.

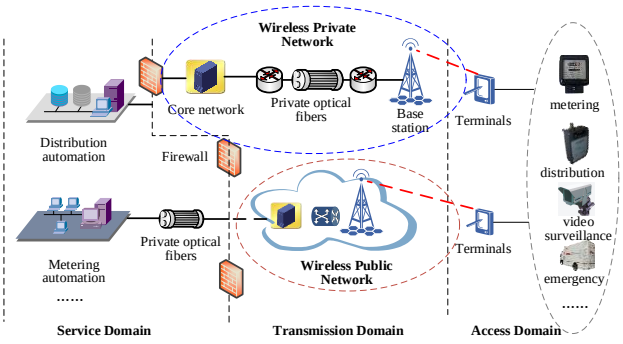

Figure 1. Wireless network architecture in power distribution network

As can be seen, both public and private wireless network utilize radio link to transmit signals from terminals to base stations, and backhaul the data from base stations to the service station through wired transmission line. The main differences between the two lie in the following two aspects: (1) Frequency spectrum: Though they may share the same radio access technology, the two networks operate on different spectrums. Public wireless network shares the spectrum with the public while the private network enjoys the dedicated use of the allocated spectrum, e.g., 1785MHz-1805Mhz or 230MHz in China. (2) Backhaul link: For public wireless network, signals are transmitted from base station to service stations through the core network of public mobile network operators. For private wireless network, signals are transmitted through the private optical transmission network.

Compared with wired network, the unique architecture of power distribution wireless network would lead to completely different characteristics in terms of reliability and security protection, thus affecting the reliable and secure operation of power distribution network.

Reliability requirements

The reliability of power distribution wireless network refers to the availability and communication performance of end-to-end transmission, which are evaluated by the parameters of bandwidth (or, peak rate), latency as well as online ratio.

As the power distribution network is developing smarter, it requires an adaptable, flexible and ubiquitous communication network, especially for the remote control and protection services[4]. However, there lacks quantified investigation and comparison on whether the bandwidth of the wireless network could accommodate the various kinds of power services, such as remote control/sensing, telemetry, video surveillance, or whether the latency and online ratio of the wireless communication link could satisfy the stringent requirements of protection and control services.

Security challenges

The security of power distribution wireless network refers to the private and exclusive use of the radio link, the confidentiality and integrity of the end-to-end transmitted data.

Either public or private wireless network employs the standard encryption and authentication methods to guarantee the secure data transmission over the radio link. However, there still exist several security challenges. For instance, USIM is the preferred initial point for attacks towards wireless network due to its stored keys and other security information. Some attacks were reported to be launched against the office network of GEMALTO, which is the largest USIM card manufacturer in the world, for the encryption key of USIM to monitor and eavesdrop the radio channels[5]. Also, the USIM card of some public mobile operators was reported to be hacked by side channel power analysis[6]. Essential encryption keys and authentication parameters were obtained during the analysis and complete duplication was achieved[7]. Meanwhile, the mobile terminals are the main sources of attacks against the wireless network. Malicious terminals could utilize stolen or duplicated USIM cards to access into the network and launch attacks against the system and other mobile terminals.

RELIABILITY EVALUATION

This section evaluates the reliability of power distribution wireless networks, including both public and private.

Communication performance

The essential parameters utilized to measure the communication performance of power distribution wireless network include the peak rate (which depends on the frequency spectrum and allocated bandwidth), latency and channel online ratio.

Table 1 shows the specific value of the above parameters of existing power distribution wireless networks being operating in CSG.

Table 1 Communication performances of different networks

	Frequency/ allocated bandwidth	Peak rate (downlink /uplink)	Latency (light/heavy load	Online ratio
Public GPRS	900MHz/ 20MHz	30kbps/ 15kbps	500ms/ 1s	95%
Public LTE	1.8GHz/ 20MHz	34Mbps/ 14.8Mbps	85ms/ 100ms	99%
Private TD-LTE	1.8GHz/ 5MHz	12.6Mbps/ 6.5Mbps	27ms/ 40ms	99.9%
Private LTE230	230MHz/ 5MHz	0.71Mbps/ 1.76Mbps	114ms/ 122ms	99.9%

As can be seen, the peak rate performance differs among different networks. This is mainly due to the differences in allocated spectrum as well as the specific radio access technology, i.e., long time evolution (LTE) as in public

LTE operating at 1.8GHz with 20MHz bandwidth, or tailored LTE as in private LTE230 operating at 230MHz with dedicated 1MHz bandwidth. Note that with the investment of public 2G network shrinking and the mobile operator's deployment of LTE towards 4G/5G, the power distribution wireless network would also evolve in the same direction.

The latency performance is determined by different access technologies and is dependent on traffic load, i.e., short latency in light load and long latency in heavy load.

The channel online ratio is dependent on whether public or private network is used, i.e., low online ratio for public network due to the shared utilization of limited resources, and high online ratio for private network due to the dedicated use of spectrum and equipment.

Service requirements

Generally speaking, there are four kinds of services in power distribution network, each of which has its individual requirements on bandwidth, latency and online ratio, as shown below in Table 2.

Table 2. Requirements of different power distribution services

	latency	bandwidth	Online ratio
Operation protection	10ms-40ms	*N**64kbps-2Mbps*	99.9%
Operation sensing and control	100ms-1s	10kbps-100kbps	99%
Management information	1s-10s	1kbps-10kbps	90%
Video surveillance	500ms	1Mbps-4Mbps	-

**N* refers to the number of protection elements.

Operation protection service: It has stringent requirement on latency due to its essential impacts on the correct operation of the power distribution network. The bandwidth requirement is also high due to its demands on the real-time transmission of the large amount of data samples. The online ratio should be near 100% due to its high reliability requirement.

Operation sensing and control service: It has relatively stringent requirement on latency, especially for remote control services. The bandwidth requirement per terminal is low due to the small amount of signalling and telemetry data transmitted. It also requires high online ratio for the on-time operations of control orders.

Management information service: It has no stringent requirement on latency, and allows retransmission. Low bandwidth and online ratio would be enough to guarantee the successful acquisition of management data.

Video surveillance: It has relatively fixed requirement on latency and occupies high bandwidth. However, there is no specific demands on online ratio since the interruption of video transmission would not impact the correct operation of distribution network.

Technical suitability

From the perspective of reliability, we obtain the conclusion on the technical suitability of power distribution wireless networks by mapping the aforementioned communication performance with service requirements, as shown in Table 3.

Table 3. Technical suitability of different wireless networks

	GPRS	LTE	TD-LTE	LTE 230	Suitable technology
Operation protection	×	×	✓	×	Private TD-LTE
Operation control	×	✓	✓	✓	All except public GPRS
Management information	✓	✓	✓	✓	All
Video surveillance	×	✓	✓	×	Private TD-LTE/ Public LTE

As can be observed in Table 3, the operation protection service demands stringent latency, high bandwidth and high online ratio, thus could only be served by private TD-LTE network operation at 1.8GHz. The operation control service could be served by public or private LTE network operating at either 1.8GHz or 230MHz due to its requirement on high online ratio and low latency. Management information service could be served by all the available networks because it has no real-time requirements on end-to-end data transmission and even allows retransmission. The video surveillance service could only be served by public or private LTE network operation 1.8GHz due to its large bandwidth consumption.

SECURITY PROTECTION

Compared to wired technologies, the radio link of power distribution wireless network is open and broadcast, which will result in the vulnerability of the transmitted information to be eavesdropped, intercepted, or tampered. Meanwhile, different from the relatively fixed location of wired terminals, the wireless ones are mobile and sparsely distributed. Lost or stolen terminals would be used as malicious station to launch illegal access and attacks toward power distribution system and other terminals.

Therefore, this section focuses on analysing the security architecture of wireless network, and proposes radio link and terminal protection methods.

Security architecture

The security architecture of power distribution wireless network is consisted of access and transmission domains. The former refers to the terminals and the radio link to base stations. The latter refers to the wired transmission line from base stations to service stations connected to the core network.

Currently, the transmission domain is protected by the virtual private network (VPN) tunnel in the core network and access point name (APN) allocated for different services, with the radio link left open and unprotected in the access domain. Meanwhile, the use of the radio link isn't controlled, either. This, however, would allow the eavesdropping and interception of the radio channel, and there exists the possibility of illegal access of malicious terminals.

Wireless link protection

As discussed in previous sections, the side channel power analysis attack threatens the security of root key *K* and other essential parameters stored in USIM. The crack of these information will result in the failure of encryption and authentication of the radio link. Towards this end, we introduce a random-noise-disturbed encryption algorithm based on the conventional 3DES encryption to handle the side channel power analysis attack.

The commonly used encryption algorithm of USIM is the 3DES, which performs data encryption standard (DES) algorithm for three times circularly. The workflow of 3DES is shown in Fig. 1:

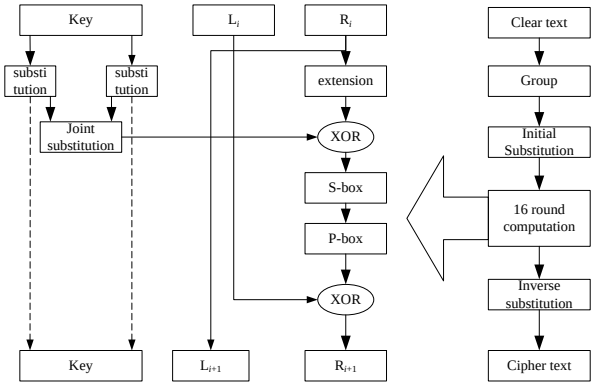

Figure 1. Workflow of 3DES in USIM encryption

As can be observed in Fig. 1, root key *K*, which is stored in USIM, is used as the parent key to generate the sub-keys of different protection levels. When attackers crack the keys used in one iteration by side channel analysis method, i.e., by observing the sharp wave of the power consumption, the overall encryption process and related keys would be obtained through statistical analysis and the wireless link would turn to be transparent to the attackers.

Herein, a random-noise-disturbed encryption method is proposed. To be specific, random computation is introduced into encryption considering the power consumption characteristics. Meanwhile, random noise is also introduced in *S*-box to disturb the location and crack of the keys. The detailed flow of the random-noise-disturbed encryption is shown in Fig. 2 and Algorithm 1.

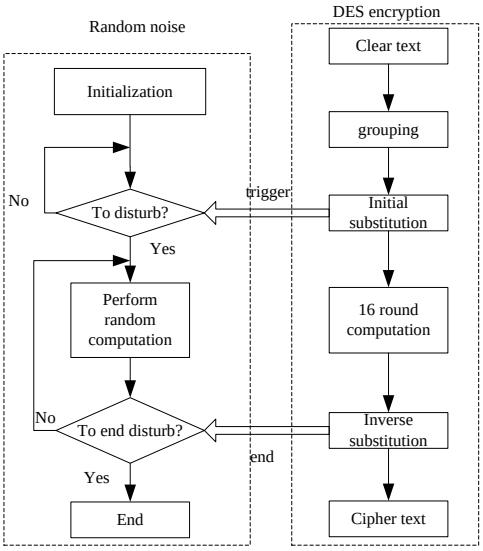

Figure 2. Workflow of the random-noise-disturbed encryption

Algorithm 1: Random-noise-disturbed DES encryption (*i*th round)

1 Divide the clear text into groups; each group contains 64 bits.
2 Make shifts of the clear text based on the IP substitution table and obtain two parts of the clear text: Right part (**R**) and Left part (**L**) with each part containing 32 bits. Random-noise in introduced in the process to disturb the actual power consumption.
3 Utilizing encryption keys and random noise to perform iterative computation for 16 rounds. The *i*th computation includes the following:
   (1). Use the **R** part of the *i*th round as the **L** part of the i+1th round
   (2). Extend and substitute the 32bit **R** part to 48bit after a random delay
   (3). Perform the operation: **R** part (xor) keys in *i*th round after a random delay
   (4). Divide the 48bit data as in (2) into eight groups of 6bit, each of which is further substituted into 4bit by S-box, thus obtaining the 32bit data after a random delay. Meanwhile, the sequence of S-box operation is also randomized
   (5). Substitution the results of (3) by P-box after a random delay
   (6). Perform the operation: results in (4) (xor) **L** part and use the data as the **R** part in i+1th after a random delay
4 Make inverse substitution based on the IP substitution table and terminate the random computation
5 Output: 64bit cipher text
6 Proceed to the (*i*+1)th round encryption

Note that the randomized *S*-box refers to the operation of adding a random delay before the *S*-box computation in the process of DES. It also introduces the random sequence of operation of the eight *S*-boxes.

Terminal protection

As mentioned before, the lack of control on the use of radio link would allow the attacks from malicious terminals. To avoid these potential security hazards, a joint authentication of USIM and terminal is proposed based on the existing 3GPP signalling process[8].

The joint authentication involves two entities. One is the terminals with joint authentication functionality, the other is the security access gateway consisted of joint authentication server and user database. The server authenticates the terminals while the database stores the

terminal and authentication status information.

The joint authentication is consisted of the following procedures: (1) authentication functionality obtains the information of IMSI/IMEI/ID of the terminal, and sends them to the security access gateway. (2) security access gateway authenticates the terminals, interrupts/blocks the transmission of malicious terminals, and configures the authentication information.

The algorithm of the joint authentication is listed below in Algorithm 2, with the workflow illustrated in Fig. 3 and Fig. 4.

Algorithm 2：Joint authentication of USIM and terminal

1 Terminal invokes the joint authentication interface to obtain the pertinent parameters
2 Terminal initiates the connection access request
3 Mobile management entity (MME) initiates mutual authentication and encryption process with the terminal
4 MME sends the *Create Session Request* message to the SAE-GW to request carrying data transmission with the joint authentication parameters
5 SAE-GW obtains the joint authentication parameters from the *Create Session Request* and forwards the *Radius Access Request* to the security access gateway
6 Security access gateway performs joint authentication
7 **If** authentication succeeds, reply *Radius Access Accept* message
  (1) SAE-GW initiates data transmission in core network and replies *Create Session Response* message to MME
  (2) MME sends *Initial Context Setup Request/Attach Accept* message to base station and terminals
8 **Else**
  (1) Security access gateway replies *Radius Access Reject* to SAE-GW
  (2) SAE-GW notifies MME of the failure of building data carrying
9 The subsequent work flow is the same with 3GPP TS23.401[8]

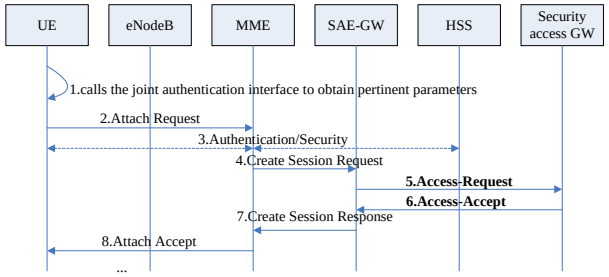

Figure 3. Workflow of admitted joint authentication

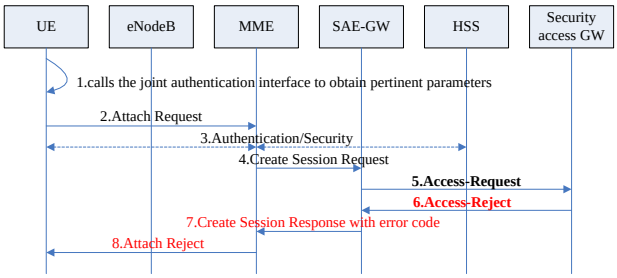

Figure 4. Workflow of rejected joint authentication

CONCLUSION

This paper investigated on the application of the wireless networks in power distribution from the perspective of reliability requirement and security protection. Technical suitability suggestions were provided by mapping the communication performance of peak rate, latency as well as channel online ratio with the practical requirements of power distribution services such as operation protection, remote control and sensing. Moreover, a random-noise-disturbed encryption scheme was proposed to overcome the side channel power analysis attack to protect the wireless link, and a joint authentication algorithm was proposed to guarantee the exclusive use of radio link by authenticated terminals.

The reliability evaluation and security protection in this paper offer quantified investigation on the technical suitability and introduce security enhancement measures, thus providing suggestions for the safe and secure application of wireless network in power distribution network.

REFERENCES

[1] Xi Fang, Misra S, Xue Guoliang. "Smart Grid — The new and improved power grid: a survey", *IEEE Commun. Surv. Tut.*, 2012, 14(4):944-980.

[2] Dong Xuzhu, Xia Qing, Rao Hong, etc. "The considerations on Smart Grid developing in China Southern Power Grid", *Southern Power System Technology*, 2012, 6(3):1-6.

[3] Jover R P, Lackey J, Raghavan A. "Enhancing the security of LTE networks against jamming attacks", *Eurasip Journal on Information Security*, 2014(1):1-14.

[4] Erol K. M, Mouftah H. T. "Energy-efficient information and communication infrastructures in the smart grid: a survey on interactions and open issues", *IEEE Commun. Surv. Tut.*, 2015, 17(1):179-197.

[5] Kaspersky Lab. "Two billion owned sim cards is a real-life nightmare", https://blog.kaspersky.com.cn/*two-billion-owned-sim-cards-is-a-real-life-nightmare/2646*, Feb 2015.

[6] WooYun. "[WooYun sumit] Crack of 3G/4G USIM cards' key and parameters", http://www.wooyun.org/*bugs/wooyun-2015-127351*, October 2015.

[7] Shaik A, Borgaonkar R, Asokan N, et al. "Practical attacks against privacy and availability in 4G/LTE mobile communication systems", *Comput. Sci.*, 2015(1), 1-15.

[8] Third Generation Partnership Project (3GPP). "LTE: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", *3GPP TS 23.401 v 11.6.0*, 2012.