文章编号：2095-4980(2025)04-0423-06

基于物联网的5G电力业务用户身份加密认证系统

曹　扬，苏　扬，陶文伟，张富川，张国翊

(中国南方电网电力调度控制中心，广东 广州 510670)

摘　要：针对传统加密认证系统认证效果差的问题，提出并设计一种基于物联网(IoT)的5G电力业务用户身份加密认证系统。硬件上，设计了加密芯片、通信器和身份识别器；软件上，利用物联网的信息传输模型，对电力业务用户的身份信息进行录入，保证身份信息的完整性；通过密码杂凑函数，计算不同数据信息的杂凑值，实现对用户身份信息的加密处理；通过终端设备生成的认证码，完成对用户身份加密的认证。通过上述软硬件的设计，完成5G电力业务用户身份加密认证系统的设计。在仿真实验中，与以往的5G电力业务用户身份加密认证系统相比，设计的基于物联网的5G电力业务用户身份加密认证系统内存泄露平均值为32 MB，认证效果更好，具有更大的应用价值。

关键词：物联网；5G电力业务；用户身份加密；加密认证系统

中图分类号：TN391　　**文献标志码：**A　　**DOI：**10.11805/TKYDA2023357

An IoT-based 5G power business user identity encryption and authentication system

CAO Yang，SU Yang，TAO Wenwei，ZHANG Fuchuan，ZHANG Guoyi

(Power Dispatching and Control Center，China Southern Power Grid，Guangzhou Guangdong 510670，China)

Abstract：In response to the issue of poor authentication effectiveness in traditional encryption and authentication systems，an Internet of Things(IoT)-based 5G power business user identity encryption and authentication system is proposed. In terms of hardware，an encryption chip，a communicator，and an identity recognizer are designed. On the software side，leveraging the information transmission model of the Internet of Things，the identity information of power business users are input to ensure the integrity of the identity information. Using cryptographic Hash function，the Hash values of different data information are calculated to encrypt the user identity information. The authentication of the encrypted user identity is completed through the authentication code generated by the terminal device. Through the above hardware and software designs，the 5G power business user identity encryption and authentication system is completed. In simulation experiments，compared with previous 5G power business user identity encryption and authentication systems，the proposed IoT-based 5G power business user identity encryption and authentication system has an average memory leak value of 32 MB，with better authentication performance and greater application value.

Keywords：Internet of Things(IoT)；5G power business；user identity encryption；encryption authentication system

电力用户身份加密认证系统广泛用于电网运行，但随着网络攻击手段层出不穷，常规的用户身份加密认证系统已不能保证用户的安全用电[1-2]。对此，不少研究学者进行相应研究，以保证用户用电信息的安全。

文献[3]提出基于高级加密标准(Advanced Encryption Standard，AES)算法的电力用户身份加密认证系统。该方法利用超混沌双向认证的原理，设计了一个身份信息加密认证模型，在AES算法的支持下，设计可认证层次化的密文策略，以实现电力用户的身份加密认证。实验结果表明，该系统的加密精确度有待提升，无法大范围应用。文献[4]提出一种基于即时感知增强算法(Artificial Intelligence-Enabled Immediate Perception Enhancement，

收稿日期：2023-11-05；修回日期：2023-12-14

AIE)模式的电力用户身份加密认证系统。在AIE模式下，处理海量繁杂的网络信息，提高网络信息的连通能力，增强系统对外界的防御能力。实验结果表明，该系统的响应时间过长，应用价值不高。文献[5]提出一种基于大数据的电力用户身份加密认证系统。该方法在大数据的支持下，设置双重密钥池，通过保护网络传输节点保证网络安全，保护用户的隐私信息。实验结果表明，该系统的身份认证效率过低。

针对上述研究的不足，本文在以往研究的基础上，提出了基于物联网的5G电力业务用户身份加密认证系统。旨在提高系统的加密精确度和认证效率，以保护电力用户的隐私信息，进而保证电网正常运行。

1 5G电力业务用户身份加密认证系统硬件设计

1.1 加密芯片

设计5G电力业务用户身份加密认证系统时，需注意加密芯片的设计[6]。本系统使用的加密芯片型号为AT91F40816，其具体结构如图1所示。该加密芯片连接了多个结构，其中，静态随机存取存储器(Static Random Access Memory，SRAM)上位机结构容量为16 kB，数据总线宽度为32 bit，可快速进行数据访问，将电网中的数据传输到加密芯片进行加密处理。其快闪(FLASH)存储器选择256 MB容量，以存储大量身份信息[7]。此外，芯片还连接了多个I/O接口，既可控制系统，又能快速访问寄存空间。在加密芯片外部，还有一个独立总线接口，用于连接多个终端控制器，确保对系统的有效控制。

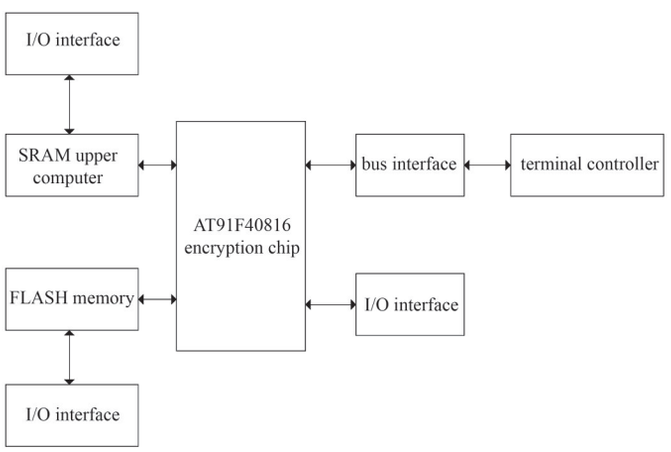

Fig.1 Structure diagram of AT91F40816 encryption chip
图1 AT91F40816加密芯片结构图

1.2 通信器

为减少电网在通信过程中的误码率，提高电网通信的稳定性和可靠性，设计一个通信器[8]，其型号为TP4B6R804，具体结构如图2所示。该通信器内部结构分为3个模块：信号接收模块主要利用通用异步收发传输器(Universal Asynchronous Receiver/Transmitter，UART)接口完成信号接收工作；信号处理模块中主要利用编码器和调制器对输入的信号进行编码，再将其放入到存储空间中，等待后续的指令；信号输出模块中，以随机存取存储器(Random Access Memory，RAM)串口为主，对处理过的信号进行高速传输，保证电网通信顺畅[9]。

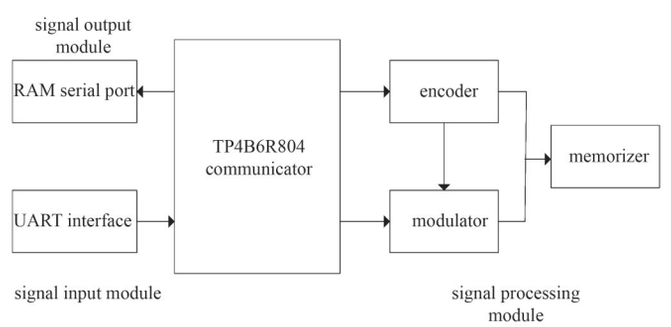

Fig.2 Structure diagram of the TP4B6R804 communicator
图2 TP4B6R804通信器结构图

1.3 身份识别器

为保证5G电力业务用户身份加密认证系统的应用效果，选用型号为BPM02的指纹识别器，其具体结构如图3所示。在识别器的内部结构中，通过指纹传感器快速采集指纹，并以数字信号处理器(Digital Signal Processor，DSP)为核心独立处理相关数据。DSP处理器具有强大的工作能力，能够在内部进行指纹比对并传输比对结果。

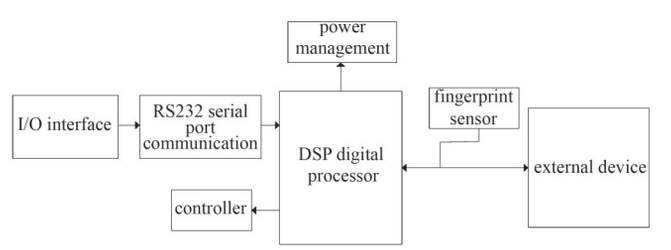

Fig.3 Structure diagram of the BPM02 fingerprint reader
图3 BPM02指纹识别器结构图

2 5G电力业务用户身份加密认证系统软件设计

2.1 基于物联网录入电力用户身份认证信息

为保证电力业务用户身份信息的完整性，设计了一种物联网信息传输模型，如图4所示。在物联网数据信息传输模型的支持下，可通过

随机获取密钥，对录入的数据信息进行匹配处理。在处理时，利用迭代顺序对单次状态序列进行密钥输出，输出前后数据的状态序列计算过程如式(1)所示：

$$\begin{cases} P_1 = f\left(IS_n, input\right) \\ IS_n = f\left(IN, input\right) \end{cases} \tag{1}$$

式中：P_1为进行迭代顺序后单次序列状态的输出值；IS_n为在某一时刻的字节数据；$input$为初始状态下的单次序列输入值；IN为物联网在该状态下的参数。通过上述计算，得到迭代后的数据内部状态。同时，结合不完整的数据集关联，将更新的映射函数描述出来，表示为：

$$\left(IS_{n+1}, P_1\right) \to f\left(IN, input\right) \tag{2}$$

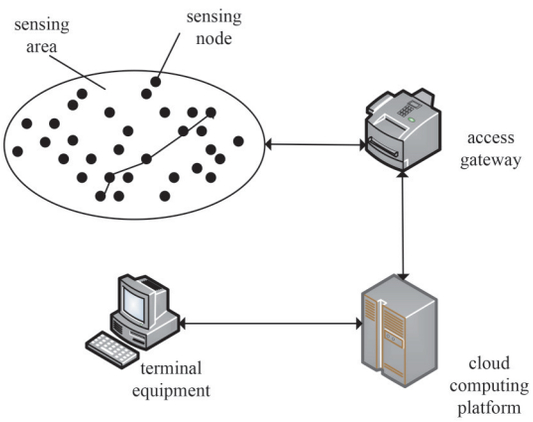

Fig.4 Data and information transmission model of the IoT
图4 物联网数据信息传输模型

式中IS_{n+1}为下一时刻采集内部序列的字节数。在利用迭代更新单次状态序列的输出值后，完成对原本数据的密钥初始化。在上述基础上，重新计算密钥的序列值：

$$K = key\left(IS_{n+1}, count\right) \tag{3}$$

式中：K为内部状态序列的密钥输出值；$count$为描述数列状态的常数项。通过式(3)将录入的用户身份认证信息进行不断更新，最终形成可被认证的标签，原本的数据状态也更新为更加机密的数据序列。至此，基于物联网录入电力业务用户身份认证信息的设计完成。

2.2 加密处理电力用户身份信息

在利用物联网完成电力业务用户身份认证信息的录入后，需通过加密算法对电力用户身份信息进行加密处理。首先，将录入的身份数据信息进行划分，构建出密码杂凑函数$H_1(Z,n)$，其中，Z表示输入的字符串，n表示输入的整数。通过构建的密码杂凑函数，计算每条输入信息的杂凑值：

$$F = \lambda P H_1(Z,n) \tag{4}$$

式中：F为输入数据的杂凑值；λ为输入数据的变化参数；P为函数识别符。

通过式(4)计算出不同数据信息的杂凑值，以此为基础，将函数的整体位数划分出来，并对其进行迭代。当迭代次数未达到规定的次数时，重复上述步骤；当迭代次数达到最大值时，利用加密算法对数据信息进行加密处理。在信息传输过程中，为防止黑客攻击，使用既定的密钥进行分析，并在正确的加密条件下保证信息传输的完整性。接收方在获得认证之前无法读取传输的数据信息，从而确保传输数据的安全性。

2.3 实现电力用户身份加密认证

在完成电力用户身份信息的加密处理后，需对用户进行身份认证。由于终端设备内部存在认证协议，设备会根据存在协议自动生成相关的认证码。认证码传输到服务器中，为之后的身份认证打下基础。通过认证码，在终端设备和服务器完成对用户身份的双重认证。使用Compare(tCode,sCode)对认证码进行比对，如果比对结果一致，则完成了对终端设备和服务器的认证；如果比对的结果不一致，则需重新认证，或更换认证信息。同时，由于设备中存在认证协议，即便设备被更换，新的设备由于缺少认证协议，也无法进行工作，自然也无法读取用户信息，从而保证了用户信息的安全性。对于在加密过程中使用的密钥种子更新很快，一旦传输的数据被截获，也无法将其破解，从而加强了数据信息的机密性。至此，基于物联网的5G电力业务用户身份加密认证系统的设计完成。

3　仿真实验

3.1 实验准备

为验证本文设计系统的应用效果，开展仿真实验。首先搭建测试平台，以Matlab为开发软件，利用阿里云服务器模拟网络环境，继而设置相关模块，具体实验参数如表1所示。

按照表1参数设置实验环境并进行实验测试，如图5所示。实验开始前，为保证系统性能，对设计的系统进

行调试。系统在调试过程中的身份认证界面如图6所示，通过此认证界面，确定系统的功能正常。同时，为保证实验过程的可靠性，选取2种对比方法开展对照实验：基于随机参数加密算法的5G电力业务用户身份加密认证系统(系统2)；基于区块链技术的5G电力业务用户身份加密认证系统(系统3)。其中，本文设计的基于物联网的5G电力业务用户身份加密认证系统设为系统1。

表1 实验参数设置

Table1 Setting of the experimental parameters

serial number	experimental parameters	experiment parameter setup
1	operating systems	Linux system(64 bit)
2	hardware environment	Intel(R)core(TM)i5−7400CPU@3.20 GHz 8 GB RAM
3	software environment	Zookeeper 3.4.10
4	development language	Java
5	working voltage/V	300
6	working current/A	50
7	working band/Hz	100

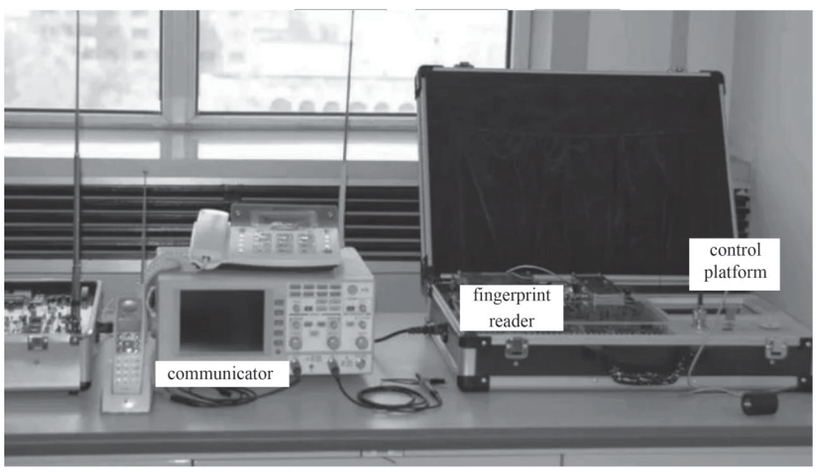

Fig.5 Setting of the experimental environment

图5 实验环境设置

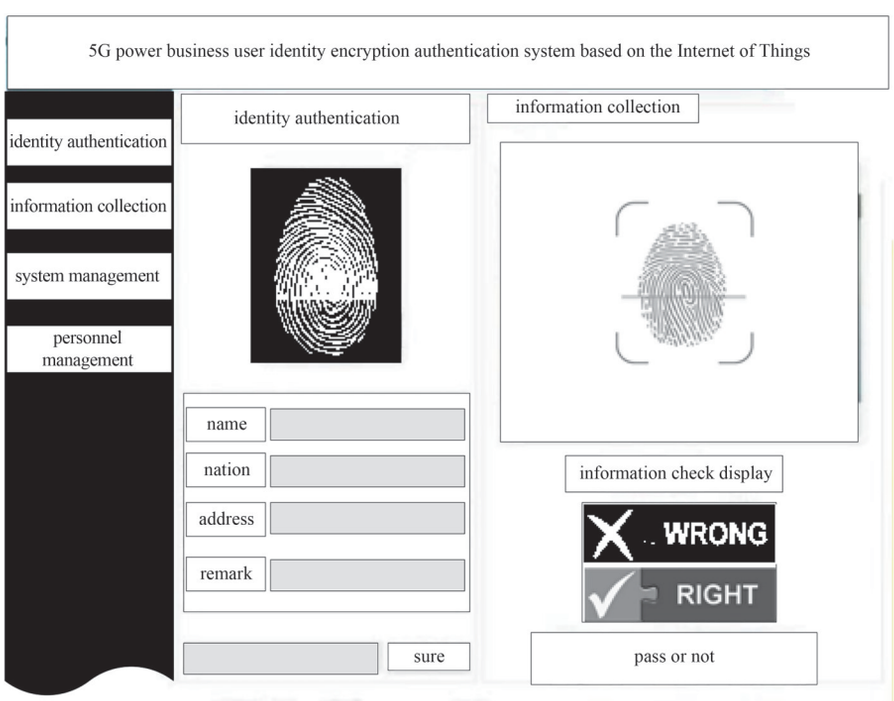

Fig.6 Interface of system identity authentication

图6 系统身份认证界面

3.2 实验结果与讨论

以系统的内存泄露情况为评价指标，对3种认证系统进行测试，对比3种认证系统的认证效果。按照设定的测试场景和用例运行3种认证系统，记录系统的内存使用情况，并利用内存分析器获取内存泄露数据，具体统计结果如图7所示。

从图7可见，身份认证的过程中，内存泄露的情况经常出现，但系统1的内存泄露远少于其他系统，内存泄露平均值为32 MB左右。由此证明，本文设计的基于物联网的5G电力业务用户身份加密认证系统的内存泄露情况最少出现，在实际应用中的认证效果最好。主要原因在于所提系统在硬件方面选择了高性能的加密芯片、通信器和身份识别器，其具有较低的资源占用和较好的效能优化，有助于减少内存泄露问题的发生；在软件方面，利用物联网的信息传输模型，对电力业务用户的身份信息进行录入并保证其完整性，确保认证系统在处理用户身份信息时没有发生数据错误或损坏等情况，从而减少导致内存泄露的潜在问题；并通过使用密码杂凑函数对不同数据信息进行加密处理，减少内存中存储敏感数据的风险。

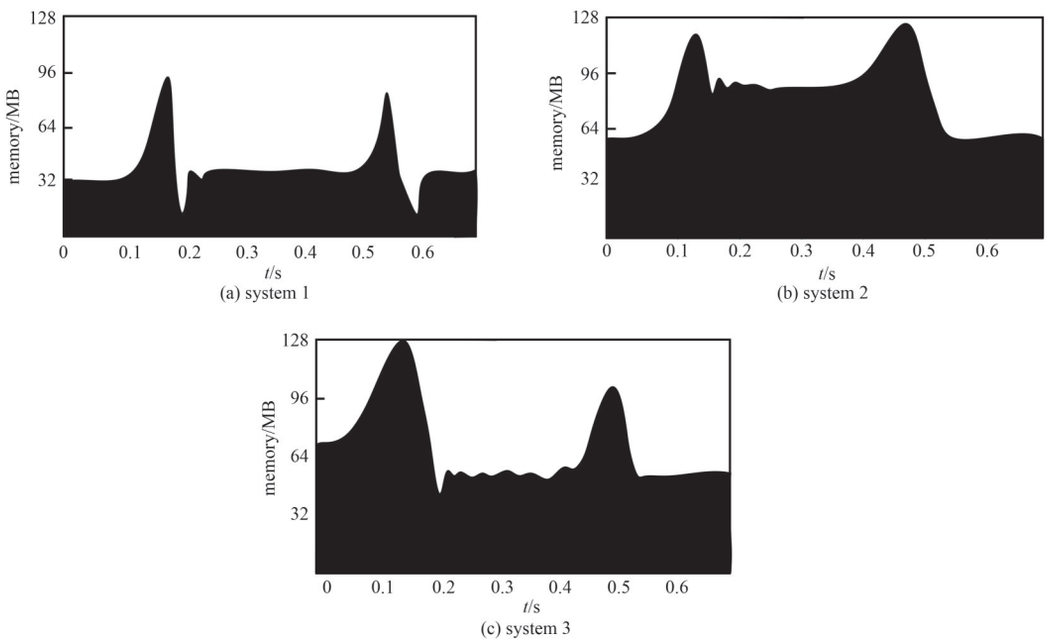

Fig.7 Memory leakage of the three authentication systems
图7 3种认证系统的内存泄露情况

4 结论

综上所述，本文设计的基于物联网的5G电力业务用户身份加密认证系统具有更强的感知能力，能够在保证用户身份信息安全的情况下实现认证。同时，本文利用密码杂凑函数进行用户身份信息加密，加密效果更好，应用价值较高。

参考文献：

[1] 段粘粘,王益义. 浅谈基于OAUTH2.0统一身份认证的多应用系统优化[J]. 电子元器件与信息技术, 2021,5(12):246–248, 250. (DUAN Niannian,WANG Yiyi. Discussion on multi–application system optimization based on OAUTH2.0 unified identity authentication[J]. Electronic Component and Information Technology, 2021,5(12):246–248,250.) DOI:10.19772/j.cnki.2096–4455.2021.12.110.

[2] 李桂琼. 基于大数据的物联网接入身份安全认证系统设计[J]. 自动化技术与应用, 2023,42(4):118–121. (LI Guiqiong. Design of identity security authentication system for internet of things access based on big data[J]. Techniques of Automation and Applications, 2023,42(4):118–121.) DOI:10.20033/j.1003–7241.(2023)04–0118–04.

[3] 谷天苓. 基于AES算法的电子通信加密认证系统设计[J]. 信息与电脑, 2022,34(15):218–220. (GU Tianling. Design of electronic communication encryption authentication system based on AES algorithm[J]. China Computer & Communication, 2022,34(15):218–220.) DOI:10.3969/j.issn.1003–9767.2022.15.066.

[4] 王鹏,厉洪瑞,王昱,等. 基于随机参数加密算法的移动互联身份认证系统的应用研究[J]. 信息与电脑, 2022,34(5):23–25.

(WANG Peng, LI Hongrui, WANG Yu, et al. Application research of mobile internet identity authentication system based on random parameter encryption algorithm[J]. China Computer & Communication, 2022, 34(5): 23–25.) DOI: 10.3969/j.issn.1003–9767.2022.05.008.

[5] 江浩. 基于AIE模式的电力物联网加密通信认证系统设计[J]. 电子设计工程, 2022,30(1):151–154,159. (JIANG Hao. Design of encrypted communication authentication system for power internet of things based on AIE mode[J]. Electronic Design Engineering, 2022,30(1):151–154,159.) DOI:10.14022/j.issn1674–6236.2022.01.032.

[6] 王晓晴,谢仪崭. 统一身份认证系统的关键设计[J]. 电信工程技术与标准化, 2023,36(4):57–63. (WANG Xiaoqing,XIE Yidi. Key design of unified identity authentication system[J]. Telecom Engineering Technics and Standardization, 2023,36(4):57–63.) DOI:10.3969/j.issn.1008–5599.2023.04.012.

[7] 张淑娥,田成伟,李保罡. 基于区块链技术的身份认证研究综述[J]. 计算机科学, 2023,50(5):329–347. (ZHANG Shu'e,TIAN Chengwei,LI Baogang. Review of identity authentication research based on blockchain technology[J]. Computer Science, 2023, 50(5):329–347.) DOI:10.11896/jsjkx.220400169.

[8] 钱泽凯,童彦澎,刘绍辉,等. 一种基于MAE人脸隐私保护方法的身份认证系统[J]. 网络安全与数据治理, 2023,42(1):15–22, 30. (QIAN Zekai,TONG Yanpeng,LIU Shaohui,et al. An authentication system based on face privacy protection using MAE[J]. Cyber Security and Data Governance, 2023,42(1):15–22,30.) DOI:10.19358/j.issn.2097–1788.2023.01.002.

[9] 鲍海燕,芦彩林. 基于改进RSA算法的隐私数据集同态加密方法[J]. 太赫兹科学与电子信息学报, 2020,18(5):929–933. (BAO Haiyan,LU Cailin. Homomorphic encryption of privacy data set based on improved RSA algorithm[J]. Journal of Terahertz Science and Electronic Information Technology, 2020,18(5):929–933.) DOI:10.11805/TKYDA2020072.

作者简介：

曹　扬(1987–)，男，博士，高级工程师，主要研究方向为电力监控系统网络安全、智能电网通信.email: lilixin337@163.com.

苏　扬(1982–)，男，硕士，教授级高级工程师，主要研究方向为电力监控系统网络安全、电力系统自动化.

陶文伟(1973–)，男，博士，教授级高级工程师，主要研究方向为电力监控系统网络安全、电力系统自动化.

张富川(1989–)，男，硕士，高级工程师，主要研究方向为电力系统通信、网络安全.

张国翊(1982–)，男，博士，教授级高级工程师，主要研究方向为电力通信.