电力负荷管理系统中数据加密技术的研究

王荣志，孙毅，冯小安，祁兵

（华北电力大学电气与电子工程学院，北京 102206）

摘要：随着电力负荷管理系统的快速发展，对网络信息安全的要求也不断提高。通过对负荷管理系统传输数据特点的分析，结合电力负荷管理系统传输规约的协议要求，提出了一套数据加密和密钥管理的方案，该方案针对各种无线通信方式的不同特点，应用不同的加密算法，对协议的各个层次进行分别加密。最后对加密方案的性能进行了分析，其结果表明该方案有效地提高了系统的信息安全性能。

关键词：负荷管理系统；加密；无线通信；数据安全

Analysis of data security algorithm for electric load management system

WANG Rong-zhi，SUN Yi，FENG Xiao-an，QI Bing

(College of Electric and Electronic Engineering，North China Electric Power University，Beijing 102206，China)

Abstract: With the rapid development of power load management system，the requirement of network information security has been improved continuously. First, the data transmission character of load management system is analyzed.Then，by taking into account the demand for power load management system data transmission protocol，this paper presents a solution for data encryption and secret key management. It takes different algorithms to encrypt each layers of protocol according to every character of wireless communication mode. Finally, the encryption solution's performance is analyzed. The result indicates that the solution has improved the information security performance effectively.

Key words: load management system; encryption; wireless communication; data security

中图分类号： TM76　　文献标识码： A　　文章编号： 1003-4897(2008)02-0054-04

0 引言

随着全国电网向现代化方向发展，为了提高电力调度自动化和电力营销管理现代化的实用水平，电力负荷管理系统的功能从控制转向管理，从限电转向服务。目前，电力负荷管理系统已具备用电监测、控制、远方抄表、防窃电分析和线损分析等功能[1]。现在的电力负荷管理系统主要采用的是无线通信方式，包括：230 MHz 数传电台通信、IS-95 CDMA 移动通信系统、通用分组无线业务（GPRS）公网通信等[2]。

采用无线通信方式，不仅可以克服有线网络存在物理环境限制的先天不足，增强系统对环境的适应性，而且能够提供良好的可移动性和可配置性。但是，与有线通信方式相比较，无线通信的信息安全问题更为突出，这是由无线通信的特点决定的：

(1)信道开放，无法阻止攻击者窃听，恶意修改并转发。

(2)无线传播会因为多种原因造成信号衰减，导致信息丢失。

(3)需要常常移动设备，设备容易丢失或失窃。

(4)用户不必与网络进行实际连接，使得攻击者伪装合法用户更为容易[3~5]。

由于以上的特点，电力负荷管理系统需要应用较高的通信保密能力。然而，现在使用各种负荷管理设备，很少采用信息安全方面的防护；即使作了加密处理，也没有结合负荷管理数据的特殊需求。本文通过对电力负荷管理系统数据传输规约的深入研究，结合当前的加密算法，提出对负控传输规约分层次进行多重加密，并根据数据传输方式的不同采用不同的加密方案，应用混合加密体制，以达到最佳的加密效果。

1 电力负荷管理系统数据加密的过程和方法

1.1 加密技术

数据加密技术是提高信息安全性能的一种有效方法。按作用不同，数据加密技术主要分为数据传输加密、数据存储加密、数据完整性的鉴别以及密钥管理技术四种[7~9]。

(1)数据传输加密技术。目的是对传输中的数据流加密，常用的方法有链路加密和端-端加密两种。前者侧重在链路上而不考虑信源与信宿，是对保密信息通过各链路采用不同的加密密钥提供安全保护。后者则指信息由发送者端自动加密，然后作为不可阅读和不可识别的数据穿过通信网络，当这些信息一旦到达目的地，将被自动重组、解密，成为可读数据。

(2)数据存储加密技术。目的是防止在存储环节上的数据失密，可分为密文存储和存取控制两种。前者一般是通过加密算法转换、附加密码、加密模块等方法实现；后者则是对用户资格、权限加以审查和限制，防止非法用户存取数据或合法用户越权存取数据。

(3)数据完整性鉴别技术。目的是对介入信息的传送、存取、处理的人的身份和相关数据内容进行验证，达到保密的要求，一般包括口令、密钥、身份、数据等项的鉴别，系统通过对比验证对象输入的特征值是否符合预先设定的参数，实现对数据的安全保护。

(4)密钥管理技术。为了数据使用的方便，数据加密在许多场合集中表现为密钥的应用，因此密钥往往是保密与窃密的主要对象。密钥的媒体有：磁卡、磁带、磁盘、半导体存储器等。密钥的管理技术包括密钥的产生、分配保存、更换与销毁等各环节上的保密措施。

1.2 负荷管理系统中的加密方式

目前电力负荷管理系统的通信方式是以数传电台通信为主，辅以其他的通信方式；结构上采取中心站、主站及从站的三级结构。网络模型图 1 所示。

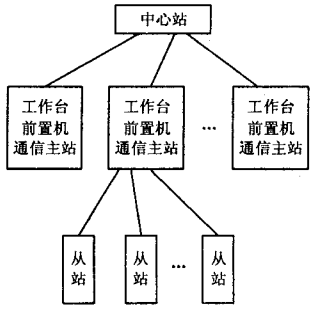


图 1 负荷管理系统通信模型

Fig.1 Load system communication model

在三层网络结构中，主站和从站之间使用无线通信方式传输数据，而在中心站和主站之间，采用电力系统的办公自动化网络进行数据传输，一般是以光纤作为通信链路的。采用无线传输方式的主站和从站之间的链路，是整个系统的通信瓶颈所在，也是系统容易遭受攻击的地方，本文研究的加密方式也以这一段链路为主。

在从站和主站的前置机之间的数据加密传输，根据不同的通信方式将采取对应的数据加密方式。

(1)数传电台通信方式下的数据加密。数传电台通信方式的组网结构简单，主站和从站之间只有一条通信链路，因此适合采用链路加密方式。为了增加数据的安全性，在数据传输之前也可以采用端到端的加密方式，将两种加密方式复合使用。当然，这是以牺牲时效性为代价的。

(2)CDMA 和 GPRS 通信方式下的数据加密。CDMA 和 GPRS 通信方式，都是通过公网运营商进行数据传输，在传输过程中要通过多条不同的通信链路[10,11]，因此不适合采用链路加密方式，改采用端到端的加密方式，数据在信道和交换节点上均以密文的形式存在。

1.3 密钥的生成和管理

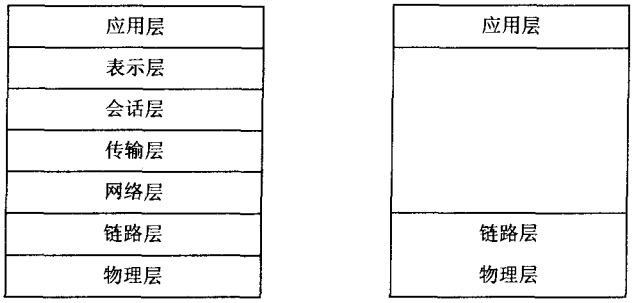
密钥的生成方式有两种：固定密钥方式和一时一密方式。固定密钥方式中，每个终端作为一个用户拥有一个密钥分配中心（KDC）生成好的密钥，主站拥有所有终端的密钥列表。而一时一密方式中，每个终端没有固定的密钥，服务器也不保存密钥。服务器根据系统安全情况，设置时间参数，定时或不定时地、自动或手动地向 KDC 请求密钥。由 KDC 将密钥送给双方。从安全角度来考虑，一时一密方式安全性更好一些，因此本文采用一时一密的密钥生成方式[12]。

在加密传输的过程中，需要大量的密钥，用以分配给主机、节点和用户。密钥的安全管理是加密通信的一个重要环节。为了降低系统的复杂性，采用中心化的密钥管理方式。KDC 负责每次加密通信的密钥的生成、分发、更新和销毁过程。参照图 1 的网络结构模型，为了给所有的主站和从站分发密钥，KDC 将配置在中心站的一台服务器上，使用集中式的密钥分配方式。

2 结合负荷管理系统数据特点的加密方案

因为电力负荷管理系统在有限传输带宽下要求特别短的反映时间，所以采用增强型的三层体系结构（EPA），如图 2 所示。与传统的 ISO 七层模型相比较，简化了层次结构，有利于数据的实时传输。

在物理层上不作数据加密，而在链路层和应用层上分别用不同的加密方式。在主站和从站的通信控制程序中分别加入针对这两层的加解密模块，而密钥管理方案在通信双方的源程序中实现。



模型 1：ISO 参考模型　　模型 2：增强性能模型

图 2 ISO 模型与负控传输模型

Fig.2 ISO model and load system transmission model

2.1 应用层的数据加密方式

图 3 是应用层帧结构，应用层协议根据功能码 AFN 的区分，将数据分成不同的类型，如确认、复位、中继站命令、设置参数、查询等。由前文的分析可知，负荷管理系统的数据对于时效性的要求各有不同，在各种数据中又根据保密性的要求分成不同的级别。因此按照 AFN 的区分采用不同的加密方式，对应用层的所有字节统一进行加密。在发送端根据级别进行数据加密，对应的在接收端进行相应的数据解密。所有的程序都是嵌入到通信控制程序之中来完成的。

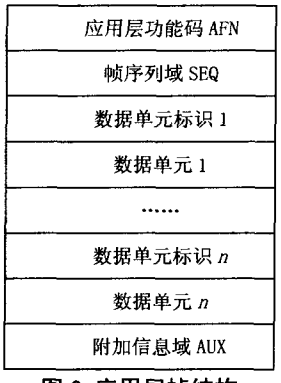


图 3 应用层帧结构

Fig.3　Application layer frame structure

2.2 链路层的数据加密方式

图 4 是链路层帧结构，链路层协议对时效性要求比较高，其中的开始字符和结束字符在传输中对于帧的开始和结束的界定尤其重要，因此不参与数据加密。对于提出报文长度、控制域、地址域及校验和等使用实时加密方案；为了提高加密速度和保密性能，对于已经加密过的应用层数据采用和链路层其他数据域相同的实时加密方案。这样，既提高对应用层数据的加密效果，同时由于链路层采用统一的加密方案，对于加密和解密的时间也作了有效的压缩，以适应这一层协议对时效性的较高要求。

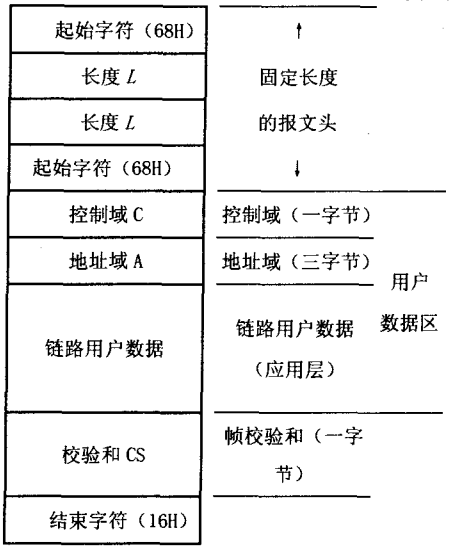


图 4　链路层帧结构

Fig.4 Data link layer frame structure

2.3 算法和密钥长度的选择

非对称加密算法安全性较高，抗攻击能力强，但是在目前存在一些工程上的缺点，如算法一般比较复杂，加解密速度慢等。因此在加密算法中普遍采用对称加密和非对称加密相结合的混合加密体制。

(1)密钥传送一般使用非对称算法，如果使用 RSA 生成密钥信息时，512 bit 在短期内仍然是安全的。但是，随着硬件设备的不断发展和攻击算法的提高，很可能不久就要采用 768 bit 或者 1024 bit 长度的密钥来保证电力系统中数据安全的需要。

(2)对称算法应用于数据的加密，速度要比相同密钥长度的非对称算法要高出一个数量级左右。因此负荷管理系统数据的加密将采用对称加密算法。常用的加密算法有 DES、IDEA 和 RC4。本文推荐使用标准长度的密钥，算法程序简单：DES 有效密钥长度 56 bit，IDEA 密钥长度 128 bit。最快速的算法是 RC4，比 DES 算法快 10 倍左右，密钥长度 40 bit。

密钥在传送过程中将采用 RSA 算法。对于链路层的数据加密将统一采用 RC4 算法。而对于应用层的加密算法，根据 AFN 来区分的加密等级，将选择不同的对称算法来进行数据加密。

3　加密方案的效果及对系统的影响

对负荷管理系统的数据进行加密，必然会带来

一定的时间开销。在有效地提高系统的安全性能的前提下，要保证不会对系统运行的时效性造成较大的影响。影响无线网络环境的实时性能的因素有：数据打包拆包，身份认证，数据加密、解密，数据的网络连接时间，网络延迟等。与不加密相比，影响响应时间的因素即身份认证和数据加密、解密的时间。身份认证的开销并不大，而对无线网络中的身份认证不必须在数据传输时进行，可以规定系统间隔一定时间即对全网的登录设备进行身份确认。因此，加密带来的时间开销可以简单的视作数据加密、解密的时间。

在加密方案中，选取了一种负荷管理终端常用的 ARM7 系列 32 位处理器 AT91FR40162，时钟频率为 70 MHz。对加密和不加密两种情况下的时间性能进行了比较。加密算法是用 C 语言进行实现的，表 1 和表 2 中的时间数值均为 1 万次随机数据的处理时间的算术平均值。实验时的无线网络传输速率为 1200 bps。

(1)CDMA 或 GPRS 通信方式，仅采用端到端的加密方式，加密算法为 RC4，表 1 中的数据长度为物理层的 1 帧的数据长度。

表 1 公网通信加密前后的对比（单位：ms）

数据长度	50 字节	80 字节	100 字节
加密前	580.940	929.515	1161.881
加密后	584.678	935.498	1169.362

(2)数传电台通信方式，采用端到端加密和链路加密的复合加密方式，为方便数据比对，两者均采用 RC4 加密算法，表 2 中的数据长度模拟用户一天的电能质量信息。

表 2 私网通信加密前后的对比（单位：ms）

数据长度	1200 字节	2400 字节	4800 字节
加密前	13942.56	27885.09	55769.97
加密后	14305.07	28665.87	57108.45

从表 1、表 2 中的数据可以看出，在 CDMA 或 GPRS 通信方式下仅采用端到端加密算法时，它加密和未加密的处理时间相差不大，加密的时间开销保持在 1%以内。而对于数传电台通信方式下采用复合加密算法时，时间开销也保持在 3%以内，同时加密强度也得到了显著增强。基本上满足了当前的系统时间要求，而且随着硬件水平的不断提高和加密算法的不断改进，数据加密和解密的时间开销还将进一步减小。

4　结束语

随着目前系统的自动化程度不断提高，对信息安全的要求也越来越高了，数据加密将是保证系统通信安全的一个重要手段，也是电力系统信息安全防护体系的重要组成部分。本文中提出的加密方案，结合了对称加密和非对称加密的优点，并且深入考虑了通信介质的影响，对不同的通信手段采用不同的加密方案。经过验证，符合电力负荷管理系统数据传输规约的要求，有效地提高了系统的安全性能。

参考文献

[1] 张峰. 电力负荷管理技术[M].北京:中国电力出版社,2005.
ZHANG Feng. Power Load Management Technic[M].Beijing: China Electric Power Press,2005.

[2] 祁兵,唐良瑞,龚钢军. 基于Mobitex的电力负荷管理系统设计[J].电力系统自动化，2006,30(5):83-86.
QI Bing,TANG Liang-rui,GONG Gang-jun. Design of Electric Power Load Management System Based on Mobitex[J]. Automation of Electric Power Systems, 2006,30(5):83-86.

[3] 夏新军,俞能海,陆铭. 针对RC4算法的无线局域网攻击[J].计算机工程与应用,2004,29:191-195.
XIA Xin-jun,YU Neng-hai,LU Ming. Attack on WLAN Based on RC4Encryption Algorithm[J]. Computer Engineering and Applications, 2004,29:191-195.

[4] 张九龙，蔡建南. 移动通信无线接入安全措施研究[J]. 江苏通信技术, 2002, 18(6) : 22-25.
ZHANG Jiu-long,CAI Jian-nan.The Analysis of Mobile Communication Wireless Access Security Tactics[J]. Jiangsu Communication Technology,2002, 18(6) : 22-25.

[5] Stallings W. Wireless Communications and Networks[M].Beijing: Publishing House of Electronics Industry,2006.

[6] 宋磊,罗其亮,罗毅,等. 电力系统实时数据通信加密方案[J]. 电力系统自动化, 2004, 28(14) : 76-81.
SONG Lei,LUO Qi-liang,LUO Yi, et al. Encryption on Power Systems Real-Time Data Communication[J]. Automation of Electric Power Systems,2004,28(14): 76-81.

[7] 贾晶,陈元,王丽娜. 信息系统的安全与保密[M].北京:清华大学出版社, 1999.
JIA Jing,CHEN Yuan,WANG Li-na.Safety and Secret in Information System[M].Beijing:Tsinghua University Press, 1999.

[8] 刘尊全. 刘氏高强度公开加密算法设计原理与装置[M]. 北京:清华大学出版社,1998.
LIU Zun-quan.Design Principles and Equipment for Liu's High Intensity Public Encryption Algorithm[M]. Beijing: Tsinghua University Press,1998.

（下转第 63 页　continued on page 63）

据容量只受物理内存和磁盘物理容量的限制，而没有设计上的限制。

6.4 用户层次上的开放

客户/服务器系统提供了客户应用程序访问服务器数据库（内存实时数据库和磁盘历史数据库）的透明接口。这个接口只包括两个函数：读数据函数和写数据函数。用户或者第三方厂家利用这个透明接口可以编写新的应用程序。所以客户/服务器系统为用户扩充新的功能提供了体系结构上的保证。也就是说，系统在用户层次上是开放的，保证系统可以不断地扩充新的功能，不但能满足用户当前的功能要求，还能满足用户将来的功能要求，做到系统永不落后。

6.5 系统维护方便

客户/服务器系统的维护，比之于分布式系统要容易得多。通常情况下只要维护系统的服务器就行了。另一方面，在任一台客户机上（包括电话拨号连接的远程工作站），都可以对服务器进行维护。

6.6 用户投资得到保护

当系统需要升级时，对客户机和服务器可以不同对待。当系统性能或者是系统数据容量不能满足要求时，只要升级服务器就可以了。客户机只是提供人机联系手段，对机器性能要求不高，不一定要求一同升级。而且，从服务器更新下来的计算机，可以继续用做客户机。这样，用户的硬件投资得到了保护。另外，客户/服务器系统允许不断地扩充新的功能，而且其数据库系统都是标准的商用数据库系统，因此用户的软件投资同样能得到很好的保护，用户以前的劳动成果可以得到有效延续。

7 结论

本文探讨了客户/服务器系统在电网调度自动化领域应用可行性和其工作原理。客户/服务器系统的工作原理可以总结为，服务器的基本任务是数据维护和数据处理，并响应客户机的请求向客户机传送格式化的数据信息。客户机则负责提供用户界面，如图形、表格以及声音、动画等。系统客户机不拥有自己的数据库（实时数据库和历史数据库），所有需要的数据及信息均取自于服务器。客户/服务器系统克服了分布式系统的许多不足，是今后电网调度自动化系统结构模式的发展方向，具有很强的生命力。

参考文献

[1] 石俊杰，孟碧波,等.电网调度自动化系统的综述[J].电力系统自动化，2004，28（8）:1-5.
SHI Jun-jie,MENG Bi-bo.Review of the Electric Power Network Dispatching Automation System[J]. Automation of Electric Power Systems,2004,28(8):1-5.

[2] 黄立红.浅谈电网调度自动化系统的发展方向[J].中国科技信息，2005.
HUANG Li-hong. Taking About Orientation of the Electric Power Network Dispatching Automation System Development[J].China Technology Information, 2005.

[3] 尚金成,等.电力市场技术支持系统设计与关键技术研究[M].北京：中国电力出版社，2003.
SHANG Jin-cheng,et al. Research of System Design and Key Technology of Electric Power Market Technology Support[M].Beijing: China Electric Power Press, 2003.

收稿日期：2006-11-17；　修回日期：2007-11-06

作者简介：
方娟妮（1977-），女，硕士研究生，从事光通信的研究；E-mail: fangjuanni@163.com
侯　伟（1979-），男，硕士研究生，从事电力自动化的研究。

（上接第 57 页　continued from page 57）

[9] 啜钢，王文博，常永宇，等. 移动通信原理与系统[M].北京邮电大学出版社,2005.
CHUO Gang,WANG Wen-bo,CHANG Yong-yu.Mobile Communication Principles and System[M]. Beijing University of Post and Telecommunication Press,2005

[10] 吴志忠. 移动通信无线传播[M].北京:人民邮电出版社,2002.
WU Zhi-zhong.Mobile Communication Radio Propagation[M]. Beijing:People's Post & Telecommunication Press,2005.

[11] 林伯钢. 网络与信息安全教程[M].北京:机械工业出版社,2004.
LIN Bo-gang.Network and Information Security Tutorial[M].Beijing:China Machine Press,2004.

收稿日期：2007-05-23

作者简介：
王荣志（1980-），男，硕士研究生，研究方向为电力系统通信、信息安全等；E-mail:ncepaps@sina.com
孙　毅（1972-），男，副教授，研究方向电力系统通信、信息安全等。