

基于GPRS 和PKI 技术的配网自动化系统

钟 晖¹ , 黄启春²

(1. 浙江省电力公司, 杭州 310007 ; 浙江大学计算机学院, 杭州 310027)

摘 要 :GPRS 通信技术不需要架设通讯线路, 组网灵活方便, 是解决配网自动化系统通信问题的有效手段。但是该方案在整个配网系统中增加了无线传输和数据中转等环节。为保证数据传输过程的安全, 采用PKI 技术为系统参与通信的前置设备和远程服务器发放数字证书, 实现安全通信。

关键词 :PKI ; 配网自动化 ; GPRS ; SCADA

中图分类号 :TM727 TM76

文献标识码 :A

文章编号 :1007 -1881(2009)01 -0005 -04

Distribution Network Automation System Based on GPRS and PKI

ZHONG Hui¹ , HUANG Qichun²

(1 Zhejiang Electric Power Corporation , Hangzhou 310007 , China ; 2 Zhejiang University , Hangzhou 310027 , China)

Abstract :It is an effective method to solve the problem of communication in distribution network automation system by GPRS , because communication via GPRS doesn't need to set up the communication line and can make networks more freely and expediently . In order to ensure data safely when transferring via GPRS , PKI is used for issuing a digital certificate to communication nodes that are preceding device and remote server .

Key words :PKI ; distribution ; network automation ; GPRS ; SCADA

0 引言

在配网自动化系统方案中, 通信系统决定了整个系统的架构、性能和投资规模, 通信系统是主站系统与配电网终端设备联接的纽带, 主站与终端设备间的信息交互都是通过通信系统完成的, 因此必须有稳定可靠的通信系统, 才能实现配电自动化的功能。通信方式有: 光纤通信、电力线载波、有线电视、GPRS /CDMA 等多种。配网自动化系统的通信具有终端设备多、单台设备的数据量小、非控制功能实时性要求不太高的特点。原有试点配网系统多采用光纤为主要通信手段, 由于配网终端分布很广, 有线方案基本上都存在投资成本很高, 维护、施工困难的问题。

为了解决原有配网自动化系统存在投入大、普及难的问题, 同时充分吸收国外的经验, 开发了基于GPRS 通信方式的配网自动化系统。采用GPRS 通信方案后系统增加了无线传输通道, 同时各终端数据必须经过无线接入系统转发, 加大了数据传输过程风险, 为保证配网系统的数据传输安全, 因此在系统设计中引入PKI 技术。

PKI(Public Key Infrastructure , 公钥基础设

施)技术就是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制, 在这一体制中, 加密密钥与解密密钥各不相同, 发送信息的人利用接收者的公钥发送加密信息, 接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性, 又能保证信息具有不可抵赖性。

同时, 为配网自动化系统中的所有参与终端和数据转发服务器发放数据证书, 在通信过程中通过加密会话, 实现系统数据传输安全。

1 系统总体结构

基于GPRS 通信和PKI 安全技术的配网自动化软件系统主要由以下7 个子系统组成, 如图1 所示。

(1)前置数据采集子系统。前置数据采集子系统安装在各变电站, 与物理设备联接, 实时采集设备状态数据, 通过内置GPRS 模块发送到中心接收转发系统, 每个前置设备都首先通过论证系统申请安全证书, 数据传输时通过加密技术与接收系统通信。

(2)无线数据转发系统。主要功能是接收

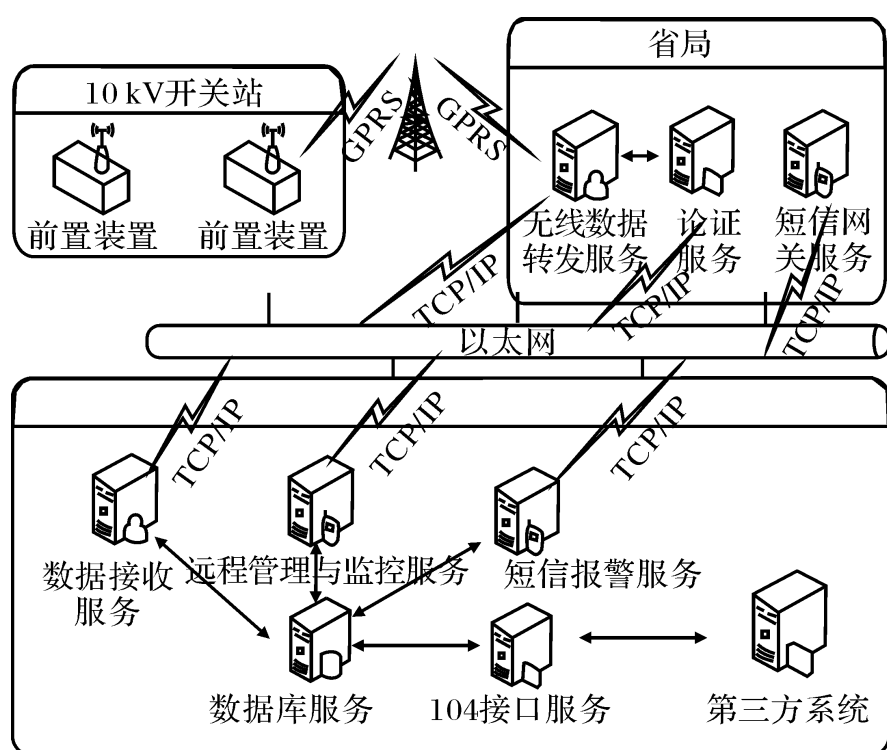


图1 系统总体结构

GPRS 终端设备数据包，进行数据包合法性验证，将数据包缓存在服务器中；系统采用多线程机制，可以支持高并发数据处理。

(3) 论证服务系统。用于为所有注册前置终端和参与通信服务器发放公钥证书，所有前置机私钥信息和公钥证书通过串口在设备注册时写入设备安全存储区，公钥信息保留在论证服务器中，除前置机外系统其它地方不再保留私钥信息。

(4) 短信通知模块。在收到 GPRS 终端发送的变位数据后，即时与系统短信网关通信，发送短信到相关设备管理者手机中。

(5) 数据接收存储模块。为保证内外网隔离，省局 GPRS 接收数据临时缓存于网关服务器中，市局数据接收服务系统定时向网关服务器请求数据，收到的数据经验证合法后按协议进行解析，并保存于数据库中。

(6) 远程数据管理及故障监控模块。该平台为 WEB 版本，用户可以通过浏览器直接访问，无需安装客户端，主要功能是实现用户管理、权限管理，站点、设备管理，监控站点设备运行状态。

(7) 104 协议数据转发模块。以 104 规约为通信接口协议，将实时数据即时传送给 DMS 系统，实现与调度系统的数据集成，既保证了系统的安全性，又能做到数据有效集成。

2 安全通信过程

基于 GPRS 通信技术的配网系统，前置机和

主站之间通过无线连接，前置机本身数量多、分布广，在整个系统通信环节中，从前置机到数据转发服务器部分是最容易出现安全问题的地方。设计时结合数字论证技术，通过加密技术实现通信安全，提供论证服务，为所有前置机发放公钥证书。论证服务、前置机、数据转发服务之间的通信过程如图 2 所示。

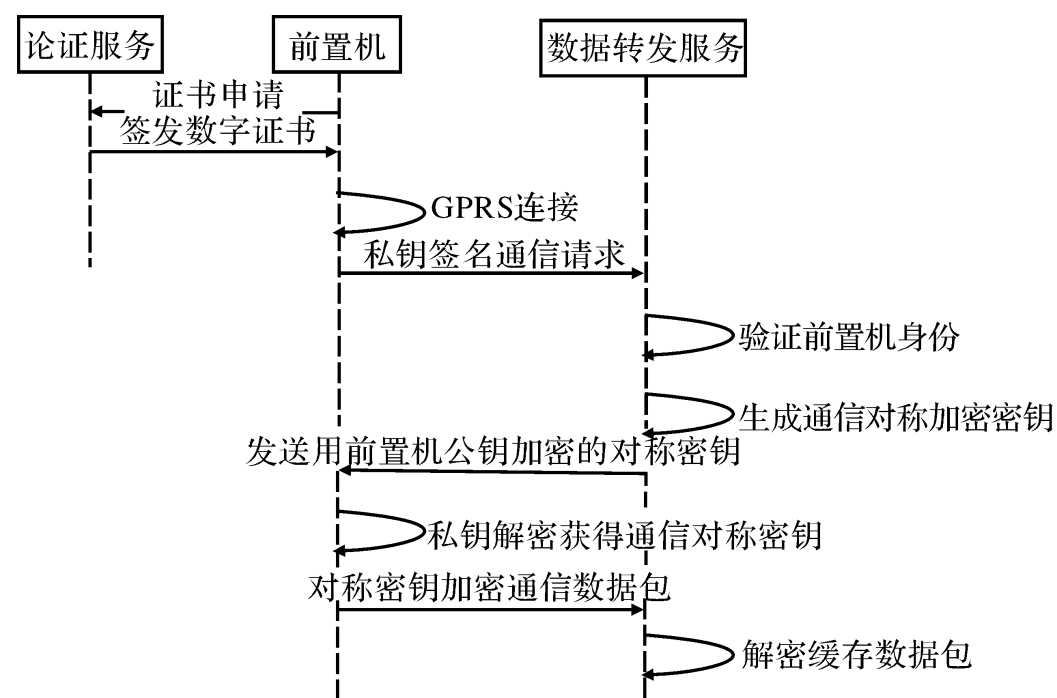


图2 安全论证通信过程

主要通信过程有以下 7 个步骤：

(1) 初始化。所有前置机安装前做初始化工作，除了纪录各种安装信息和参数外，还要向论证服务器申请公钥证书，公钥证书和私钥通过串口写入前置机安全存储区，这样每台前置机就有了唯一的安全身份保障。

(2) 前置机发起通信。先拨号获得 GPRS 通信连接，连接成功后向数据转发服务器发送经过前置机私钥签名的连接请求数据包。

(3) 数据转发服务器收到数据包后，使用公钥证书验证前置机身份合法性，未经合法论证的数据包将被丢弃。

(4) 前置机请求验证合法后，数据转发服务器生成通信用对称加密密钥，并将该密钥用前置机的公钥进行加密后返回给前置机。

(5) 前置机收到数据包后用自己的私钥解密，得到与数据转发服务器的通信对称密钥。

(6) 前置机对发给转发服务器的数据包用通信对称密钥加密后发给服务器。

(7) 服务器收到数据包后用对称加密密钥解密后缓存数据包，等待处理。

以上是完成一次前置机和数据转发服务器之间通信的过程，前置机在每次重新建立连接时都

要进行新的通信请求, 接收服务器也会重新生成通信对称密钥, 前置机请求被破解的可能性基本没有。

3 模块功能分析

系统模块间逻辑关系如图3所示, 其中无线数据转发模块、安全论证模块、短信通知模块、数据接收存储模块, 在前面子系统功能描述中已有说明, 下面主要介绍远程数据管理及故障监控模块和SCADA 数据接口模块。

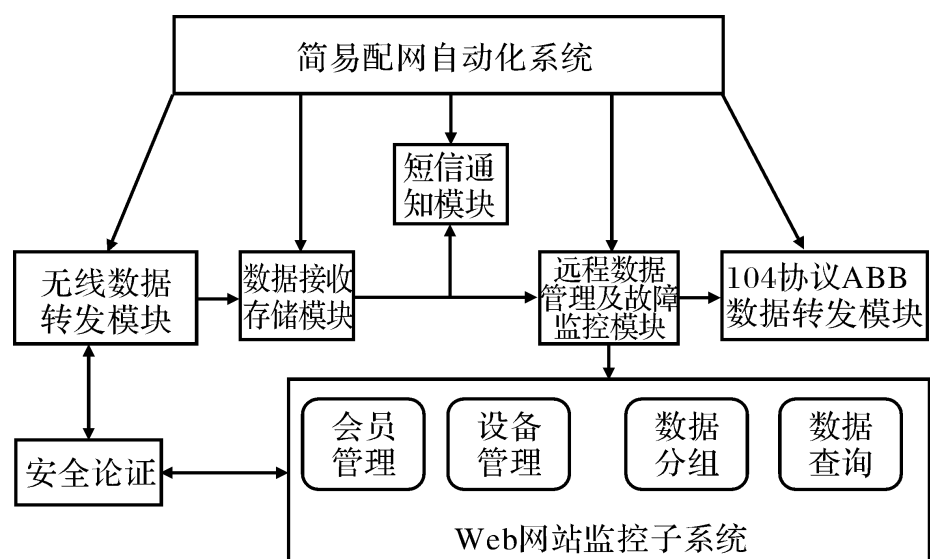


图3 系统模块图

3.1 远程数据管理及故障监控模块

这是一个相对独立的模块, 是通过BS 模式实现的一个网站应用系统, 主要提供管理站点及设备数据, 提供查询、监测站点实时数据的各种功能。此模块又可划分成几个小模块, 如图4所示。

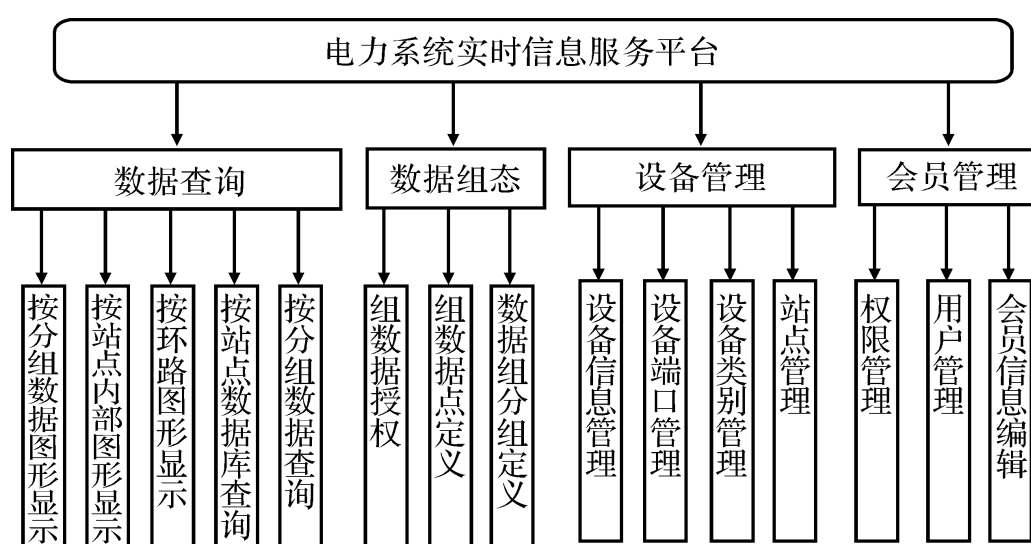


图4 主站管理监控系统功能结构

(1) 会员管理。对系统用户进行增、删、改等操作, 管理系统用户及权限的分配。

(2) 设备管理。动态分配各个站点的设备, 注册管理数字证书及设备端口的分配。

(3) 数据分组。定义数据分组, 一个数据分

组可以包括多个站点, 为数据分析监控提供分类。

(4) 数据查询。按动态、静态多种方式查询数据, 形象地查询监控站点实时数据。

3.2 与SCADA 数据集成模块

本系统实现了SCADA 服务接入接口, 用来将数据信息转发给SCADA 服务系统, 严格按照104 协议进行数据通信, 并实现了数据的同步实时。

3.2.1 数据结构

整个通信过程中, 都是以数据包的形式进行数据的转发、接收以及处理。同时对数据包重新进行构造和解析, 有几个贯穿整个系统的主要数据结构, 通信数据包结构以101 协议为基础。

3.2.2 算法

(1) 接收线程算法流程如图5所示。其中nBuf 为从网络中读到数据的缓冲区; nBufRecv 为缓冲区, 其长度为LEN, 用它来判断有没有接收到报文; nPosW 为写指针; nPosR 为读指针。对nPosW、nPosR 的任何一次操作, 均要作如下判断:

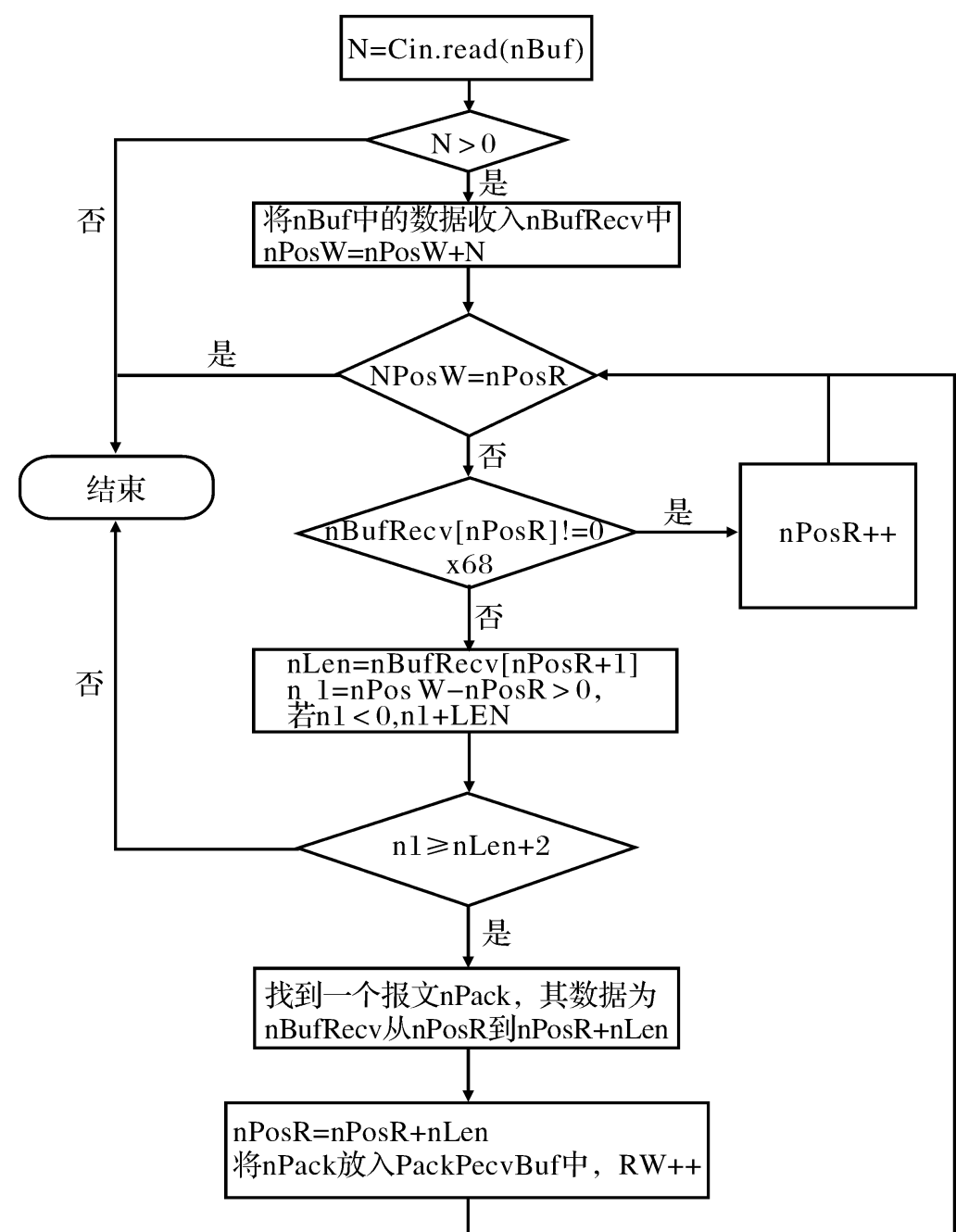


图5 数据接收线程流程图

“ If nPosW > LEN then nPosW = 0 ” 或 “ If nPosR > LEN then nPosR = 0 ”。

(2) 数据处理算法流程如图6 所示。

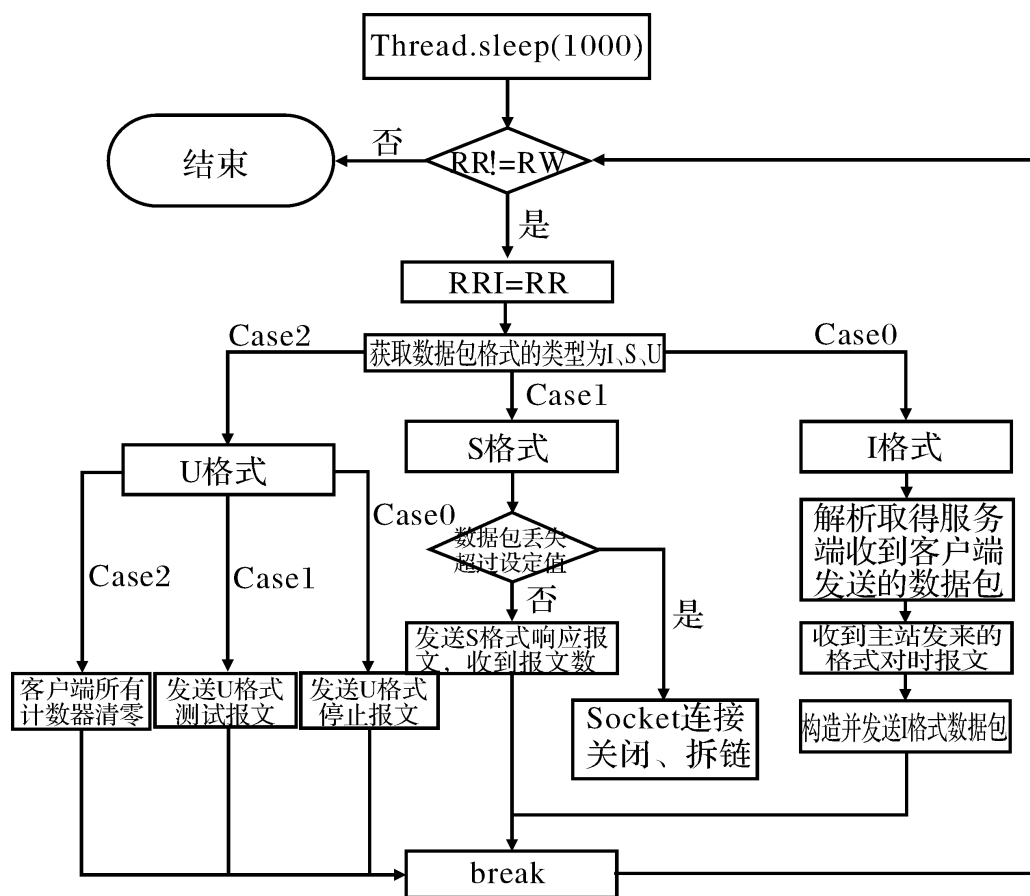


图6 数据处理线程流程图

4 系统特点

基于GPRS 通讯方案和PKI 安全技术的配网自动化系统主要有以下优点：

(1) 前置装置充分利用现场已经安装的故障指示仪输出信号，不用重复投入设备，降低了前置装置成本。

(2) 通信方式采用GPRS 传输，解决了传统光纤通信带来的布设难度大、安装工期长、成本高的问题。

(3) 通过PKI 技术保证所有信息传输过程的安全性。

(4) 主站采用WEB 平台，方便远程访问监控设备状态。

(5) 结合短信通知系统，给设备维护人员提供及时的信息服务，大大降低了设备巡查的工作，提高设备异常信息处理的速度。

(6) 采用104 通道与SCADA 系统接口，既保证系统的数据实时性，同时又有效隔离系统的相互影响，保证调度系统的安全。

系统的不足主要体现在以下2 个方面：

(1) GPRS 通信方式实时性没有光纤通信方式好，目前系统以上行数据为主，下行不作控制。

(2) 前置装置利用原有的故障指示仪，采集的数据受故障指示仪输出信息的精度和数量的限制，无法采集到更多的其它数据。

经过一年多时间的试运行，系统运行稳定，每个站点平均系统投资只有传统方案的1/5 左右。系统安装实施方便，不存在光纤铺设需要协调市政等多方面关系的问题，目前系统主要采集故障指示数据，下一步需要考虑接入更多的信号类型，增强主站对数据的分析功能，提供更有效的辅助决策能力。

5 结语

无论是城市配网改造，还是在县级配网建设中，基于GPRS 和PKI 技术的配网自动化实施后都具有自动化水平高、供电可靠性高、功能强、实时性好、适应电力市场需要等技术特点，同时又具有维护费用低、节能、节资等显著的经济性。所以，在条件成熟的县级配电网中积极采用、推广配网自动化具有重要的现实意义。而采用GPRS 和PKI 技术，则为配网自动化的应用提供了技术支持。

参考文献：

- [1] 王明俊，于尔铿．配电网自动化及其发展[M]．北京：中国电力出版社，1998．
- [2] 孙际明，孔泽明，张小水．一种电能计量管理系统的设计[J]．电力系统自动化，1997，21(12) 51-53．
- [3] IEC 1334．Distribution Automation Using Distribution Line Carrier Systems[S]．1998．
- [4] Newbury J．Communication Requirement and Standards for Low Voltage Main Signaling[J]．IEEE Transactions on Power Delivery，1998，13(1)．

收稿日期：2008 -11 -10

作者简介：钟 暉(1971 -)，男，浙江缙云人，高级工程师，主要从事城市电网建设与改造工作。

(本文编辑：陆 莹)

发展经济

电力先行