基于无线双网关的移动应急电力远动系统设计

袁永军

(杭州市电力局，杭州 310009)

摘要：随着智能电网概念的提出，如何采用多种通信介质建设快速、经济的远动通信平台成为研究热点。GPRS 无线通信模式相比传统的有线通信具有显著的成本效益和灵活的组网能力，因此提出基于无线双网关的移动应急电力远动系统方案。该系统通过自适应通信网关实现通信规约的自适应转换，采用远动安全网关确保无线通信信息传送的安全性。

关键词：GPRS；通讯；网关；远动；虚拟专用网

中图分类号：TM762 **文献标志码**：B **文章编号**：1007-1881(2010)08-0045-04

Design of Mobile Emergency Telecontrol System Based on Wireless Dual-gateway

YUAN Yong-jun

(Hangzhou Municipal Power Supply Bureau, Hangzhou 310009, Zhejiang)

Abstract: Along with the proposed concept of intelligent power grid, how to adopt multiple communication media to build a rapid and economical telecontrol communication platform system becomes a hot topic. GPRS wireless communication mode has apparent cost benefits and agile networking capability by comparison with traditional wired communication. Therefore, this paper proposes the plan of mobile emergency telecontrol system based on wireless dual-gateway which uses self-adaptation communication gateway to realizes self-adaptation conversion of communication protocol and ensures the safety of wireless communication information transmission by telecontrol security gateway.

Key words: GPRS; communication; gateway; telecontrol; VPN

电力远动系统的组网方式大量使用了载波、微波、光纤等固定通信通道的形式。随着建设智能电网[1](Smart Grid)的步伐不断加快，远动系统中固定通信通道暴露出明显的不足，如部分电网基建工程在有线通道未建立时，已经有数据传输的需求；而地震、暴雪等自然灾害，很可能对固定通信通道的正常运行产生严重影响。

相比有线通信模式，无线通信模式具备更高的成本效益，更灵活快捷的组网能力，在电力系统中的应用研究引起了广泛关注[2-5]。同时，为满足建设智能变电站的要求，远动通信将逐步采用国际标准的 IEC 61850 通信规约，而现有变电站通信规约种类繁多，需要规约转换工具实现规约的标准统一。因此，为了保证在全天候、多种条件下电力数据的安全有效以及无缝化传输，提出基于无线双网关的移动应急电力远动系统方案。

1 远动系统通信模式探讨

目前远动系统大多采用 RS-422 和 RS-485 串口传输或现场总线网，无论采样串口传输还是现场总线网络传输，其介质都是有线的，都要受布线的限制，特别是要把相距较远的节点连接起来时，敷设专用通信线路的布线施工量大、费用高、耗时长，不利于网络的升级、扩展。无线通信模式(如 GPRS)以公共电磁波为通信信道，因其施工维护简单、安装费用低、建设周期短、组网灵活等优点，可弥补远动系统中有线通信模式的不足。

但是，无线通信模式也存在安全系数低、易受干扰、通信延时长等缺点。要在远动系统中采

用无线通信模式，必须保证信息传送的安全性，即数据传输满足二次系统安全防护的要求，实现信息的认证和加密。同时，为解决无线数据传输的抗干扰和时延问题，利用冗余通信技术和规约校验与重传技术，优化数据传输机制，保证数据传输的可靠性和实时性。

基于无线网络的移动应急远动系统需要突破原有的体系结构和传输模式，在充分利用无线网络的基础上结合最新的网络化规约、数据安全加密技术，才能实现无线网络环境下调度中心与变电站之间快速、灵活、准确、安全的信息交互。IEC 61850 是国际最新的变电站自动化通信协议，加快其在变电站自动化产品中的实施与推广已经成为广泛共识。然而，当前变电站有大量遗留设备并不支持 IEC 61850 规约，因此，开发针对遗留产品的规约转换通信网关是实现电力数据无线全景通信的前提。同时，为保证电力调度数据通过无线网络传输时的安全性，可借助基于 IPSec 协议[6]的虚拟专用网 VPN[7](Virtual Private Network)安全网关技术对数据的传输进行安全防护。

2 应急远动系统结构设计

2.1 信号传输

在远动通信各个系统之间转发数据时，经常遇到双方规约不一致的问题，而系统自适应通信网关支持大多数远动规约(如 DNP3.0、IEC 101、IEC 104、TASE.2、IEC 61850 等)，可以方便实现规约转换，将通过某种规约接收到的数据，通过 IEC 61850 规约直接转发出去，不影响传输的速度和效率，既可以全部转发也可以选取部分转发，配置方便。

规约统一后的报文数据通过串口和远动安全网关相连，避免公网的非法信息侵害变电站和调度中心自动化运行设备。变电站侧远动安全网关将报文数据打成 IP 包，并经过 IPSec 协议二次加密，再通过无线发射终端传到 GPRS 网，最后通过调度中心侧远动安全网关解密并使用串口通信到达前置通讯机。

2.2 无线通信组网方式

GPRS(General Packet Radio Service)技术是在原有 GSM 网络结构中增添 3 种新的网络节点，即分组控制单元(PCU)、GPRS 业务支持节点(SGSN)和 GPRS 网关支持节点(GGSN)以及对 GSM 的相关部件进行软件升级来实现。GPRS 采用时分多址(TDMA)方式传输话音，用分组方式传输数据。GPRS 支持 TCP/IP 协议和 X2.5 协议，在 GPRS 上可以开发基于 IPSec 协议的虚拟专用网 VPN 和访问点域名 APN(Access Point Name)业务。

采用 GPRS 组网的详细网络结构如图 1 所示，在控制中心侧用内网 APN 专线方式连接，即从电信公司后台服务器引出 2M 的 DDN 专线与调度中心远动安全网关连接，由电信公司提供固定 IP 地址；在变电站侧采用固定 IP 地址的 SIM 卡通过远动安全网关的无线发射终端接入 GPRS。该 APN 为电力公司专用 APN，对访问接入范围进行了严格的限制。将 APN 与终端静 态 IP 地址绑定后，只有特定终端 IP 地址才可访问 APN。如果需要增加该 APN 的设备，必须由电力公司出具授权书，委派移动公司另行开卡接入，确保该 APN 的安全性。采用该组网方式的数据安全性好，稳定可靠，传输延迟小，能满足大部分报文传输的实时性要求。

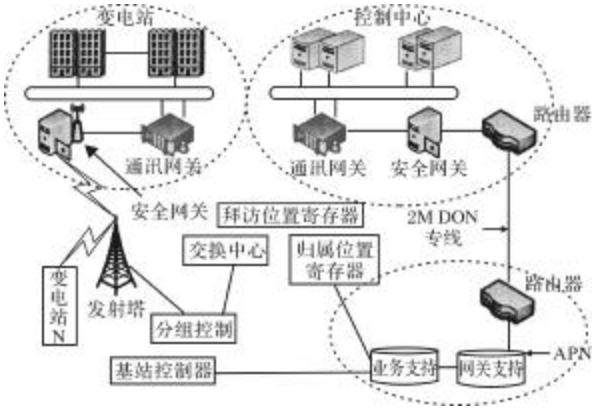

图 1 无线通信详细组网方式

2.3 远动安全网关设计

无线远动通信系统的变电站侧和控制中心侧分别处于两个独立的子网，其内部网络的主机不负责加密工作，系统采用基于 IPSec 协议的 VPN 隧道模式在安全网关之间建立安全通道(如图 2)。两个安全网关分别保护位于后面的子网，通过 HTTPS 加密通讯数据协议访问安全网关服务器，经过身份认证后，设置网关的安全策略，安全网关控制中心侧为主设备，其远程设备后方子网设置为变电站侧的 IP 段，安全网关变电站侧从设

备的远程设备后方子网设置为控制中心侧的 IP 段。安全网关的出口 IP 地址设置为无线 GPRS 网络专网静态地址。通过这样的安全配置对接入访问的范围和资源进行限制，两个子网之间传输的数据都是经过两个安全网关协商处理过的加密和认证的数据。信息在网关之间的专有隧道上传输，保证了数据在公共网络上的传输安全，从而构成有安全保证的 VPN。即使外部用户非法获取这些数据，也不会对源主机或网络形成威胁。

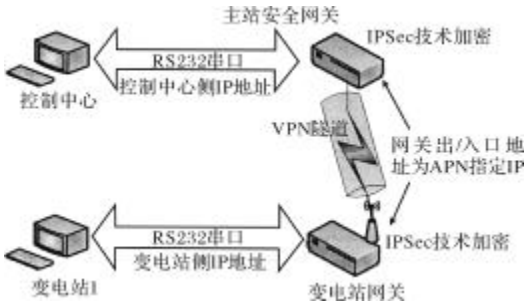

图 2　VPN 隧道通信

IPSec 安全认证技术是在网络层上对数据包进行安全处理，从而提供数据源验证、无连接的数据完整性、数据机密性、抗重播和有限的业务流机密性等安全服务。IPSec 体系是一个开放的标准框架(如图 3)，包括 3 个主要的安全协议，即认证头协议 AH(Authentication Header)、封装安全有效载荷协议 ESP(Encapsulating Securit Payload)和密钥交换协议 IKE（Interne Key Exchange)。IPSec 的安全服务由通讯双方建立的安全关联(SA)提供，由其选择由 ESP 还是 AH 来保证 IP 上的传输，IKE 负责 SA 的协商及密钥交换。

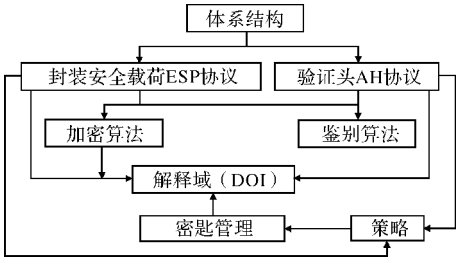

图 3　IPsec 体系结构

在这个 VPN 中，每一个具有 IPSec 的安全网关都是一个网络聚合点，试图对 VPN 进行信息内容分析将会失败。目的地是 VPN 的所有通信，都经过安全网关上的 SA 来定义加密或认证的算法和密钥等参数，即从 VPN 的安全网关出来的数据包只要符合安全策略，就会用相应的 SA 来加密或认证(加上 AH 或 ESP 包头)。所有的加密和解密由两端的安全网关全权代理。

(1)发送方 IP 分组的处理过程：源主机发送一个 IP 分组给安全网关，安全网关针对 IP 分组目的地址查询策略引擎，根据安全策略强制加上 AH 或 ESP 头，对没有 SA 的安全策略利用 IKE 建立新的 SA，安全网关发送这个经过 IPSec 处理过的分组。

(2)接收方的处理过程：另一端的安全网关收到这个分组，利用分组的 AH 或 ESP 头调用 IPSec 处理，进而决定 IPSec 处理的应用是否正确，如果验证正确，那么解密恢复到原始数据分组并转发到真正的目的主机。

3　自适应通讯网关设计

自适应通讯网关主要包括以下 4 个功能模块：数据模型映射模块、动态规约转换模块、实时库模块、ACSI/MMS 服务模块。通信网关软件结构如图 4 所示。

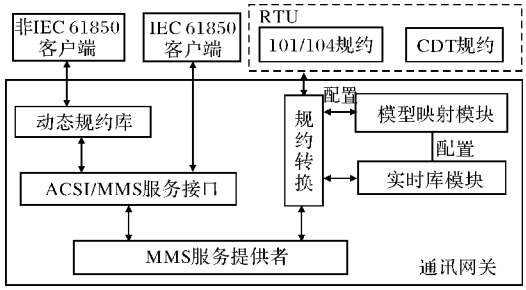

图 4　通信网关软件结构

3.1　数据模型映射模块

为了使通讯网关能够成为不同遗留产品的通用封装器，必须对电力对象提供统一的数据模型。本系统采用 IEC 61850 的建模方法，并在此基础上扩展，完成了变电站系统的数据模型扩建，并对其进行元数据和元数据映射服务。通过元数据所描述的信息，网关中协议转换器的结构在运行期得到配置，虚拟实时库建立遗留产品的通用数据模型。通过模型映射，协议转换器能完成不同协议间的自动适配。

3.2　动态规约转换模块

非 IEC 61850 协议的数据模型都面向信号，对 RTU 的信息描述都是以点表的形式，从逻辑上看是线性和平面的，而 IEC 61850 的数据模型是面向对象的、分层和立体的。因此将传统远动协议转化为 IEC 61850 协议，首先是线性信息如类型标识符、可变结构限定词、传送原因、应用服务数据单元公共地址和功能类型等，从 101/104 所定义的应用服务数据单元(ASDU)到 IEC 61850 中面向对象信息(服务器、逻辑设备、逻辑节点、数据对象和数据属性等)的转化过程。其次，是将 IEC 60870-5-101/104 等规约的服务映射到 ACSI 服务。

为了实现灵活快速的规约转换，为现存的大多数远动规约（CDT、DNP3.0、IEC101、IEC104、DL476、TASE.2、IEC61850)提供标准接口，每个规约为一个动态库，能够按需添加新规约而不影响系统的运行。通过一种规约接收数据，识别提取数据包中的有效信息，经过元数据管理将其映射到虚拟实时库中，再通过规约转换模块生成需要的规约转发出去。

3.3 实时库模块

实时数据库是内存数据库，选择文件映射方式实现高效可靠的内存管理。由于变电站设备模型的总体结构是按逻辑设备、LN、数据对象划分的层次结构，因此选择基于层次模型的实时库产品。同时，对子站监控系统的实时库进行映射，并统一进行管理。通讯网关实时库可以将多个厂站的数据归一，以统一的链路发送给调度；同时调度的数据可以复制到多个链路发送给多个厂站。当发生雷暴等恶劣气象条件造成 GPRS 通信中断时，一方面归一化数据将在实时库的预留存储空间保留，并及时给出报警，以防止长期故障而引起预留空间存储数据的溢出；另一方面通过自动重连功能尝试拨号接入网络，利用断点续传功能将保留数据发送出去，保持数据传输的连续性。

3.4 ACSI/MMS 模块

IEC 61850 总结了电力生产过程特点和要求，归纳出电力系统所必需的信息传输的网络服务，采用抽象建模方法设计出 ACSI，它独立于具体的网络应用层协议，与采用的网络无关。ACSI 服务是一种抽象通信服务，必须将其映射到具体的通信服务，对携带服务参数的报文格式和编码规则以及网络传输方式加以定义，才可以用于实际的信息交换过程。MMS 定义了一套标准的服务，MMS 用户使用相同的服务进行交互，从而实现互操作性。

4 结语

本文提出的基于无线双网关的移动应急远动通信系统方案，解决了基建工程通信、电网故障通信等短期应急通信问题。为保证无线通信符合二次安防要求，在变电站及调度中心入口皆采用串口通信，通过基于 IPSec 安全协议的 VPN 隧道模式建立虚拟专用网实现外网隔离，采用接入点域名服务 APN 提供 GPRS 专有信道。同时运用最新的 IEC 61850 通信规约，满足未来智能变电站的通信需求。限于无线通信技术在通信带宽、通信速率、系统稳定性和安全性等方面固有缺陷的影响，无线通信模式还不足以取代有线通信在电力系统远动通信中的地位，但随着无线通信技术的不断发展，其在电力系统远动通信中的应用范围将更为广阔。

参考文献：

[1] 肖世杰.构建中国智能电网技术思考[J]. 电力系统自动化, 2009,33(9):1-4.

[2] 唐海军.基于 GPRS 的配电网馈线自动化模式探讨[J]. 电力系统自动化,2006,30(7):104-107.

[3] 李惠宇,罗小莉,于盛林.一种基于 GPRS 的配电自动化系统方案[J].电力系统自动化,2003,27(24):63-65.

[4] 所旭,张萍.无线通信技术应用于变电站自动化的探讨[J].电力系统自动化,2004,28(17):88-91.

[5] 黄新波,刘家兵,王向利,等. 基于 GPRS 网络的输电线路绝缘子污秽在线遥测系统[J].电力系统自动化,2004,28(21):92-96.

[6] 唐佳佳,周晓东,陆建德. IPsec VPN 安全网关的认证优化设计与实现[J].计算机应用与软件,2008,25(5):59-61.

[7] BROWN S. 构建虚拟专用网[M]. 董晓宇,魏鸿,马洁,等译. 北京:人民邮电出版社,2000.

收稿日期：2010-03-09

作者简介：袁永军（**1974-**），男，浙江绍兴人，工程师，从事电网建设管理工作。

（本文编辑：杨 勇）