

电力移动作业 PDA 安全接入系统设计与实现

秦 超, 张 涛, 林为民

(中国电力科学研究院, 江苏 南京 211106)

摘 要: 本文分析了传统电力移动作业 PDA 接入系统可能存在的安全风险, 设计和实现了更为安全的接入系统, 对其总体架构及功能进行了详细分析。该系统可进行双向证书认证、数据保密传输、安全访问控制、网络隔离与安全数据过滤、实时监控管理, 可有效解决电力移动作业应用的安全防护问题。

关键词: 电力移动作业; 个人数字助理; 安全接入系统; 通用分组无线服务/码分多址; 安全数码加密卡; 公钥基础设施; 双因子认证; 安全隔离过滤; 实时监控审计

0 引言

目前, 电力系统已逐渐采用个人数字助理(PDA)^[1]通过GPRS/CDMA无线公网接入电力生产、营销、物资、应急指挥等内网业务系统以开展移动作业应用^[1]。该方式相比传统作业纸质填写方式, 在作业效率、质量、规范性等方面有很大提高, 但也存在一定的安全隐患, 如身份认证、数据安全传输、终端监控管理等, 目前还未有完善的解决方案。本文对上述安全问题进行了详细分析, 并进行了安全接入系统总体功能架构及接入流程设计以克服上述安全风险。

1 电力传统移动作业PDA接入系统安全性分析

电力传统移动作业PDA接入系统的主要系统架构可概括为由移动作业人员持有PDA终端, 经由GPRS/CDMA无线网络经专线访问点(APN)^[2]进行无线拨号接入, 并基于用户名、口令进行终端身份验证。其主要安全隐患分析如下:

(1) 身份认证强度低

手机号绑定特定APN网络, 经GPRS网络服务节点(GGSN)^[2]接入不能解决手机号码伪造问题, 同时用户名口令验证强度较低。

(2) 传输通道安全性差

使用APN专线接入, 经由无线PDA终端→基站→GPRS服务节点(SGSN)^[2]→GPRS网关节点(GGSN)→专线路由器→APN专线接入路径, 无线PDA至SGSN传输数据进行了加密, SGSN至电力网络进行专线传输, 由于主流无线加密算法(如A5/1, A5/3等)的脆弱性^[3], 传输通道安全性无法有效保证。

(3) 网络隔离强度弱

未进行电力信息网络与公网信道间的双向安全隔离及数据过滤^[4], 网络边界路由器、防火墙等不能完全确保核心内部网络安全。

(4) 终端集中监管及访问控制难

各移动作业子系统相互独立, 信息无法重用, 难以进行精细监控及管理, 维护成本高, 易造成安全隐患。

(5) 终端行为安全审计难

对终端访问行为如上传、下载、接口访问等很难进行实时监控及细粒度地安全审计。

以下结合电力系统实际, 引入一些关键技术进行电力移动作业 PDA 安全接入系统的安全架构设计, 以解决上述安全问题。

2 电力移动作业PDA安全接入系统设计

2.1 逻辑结构设计

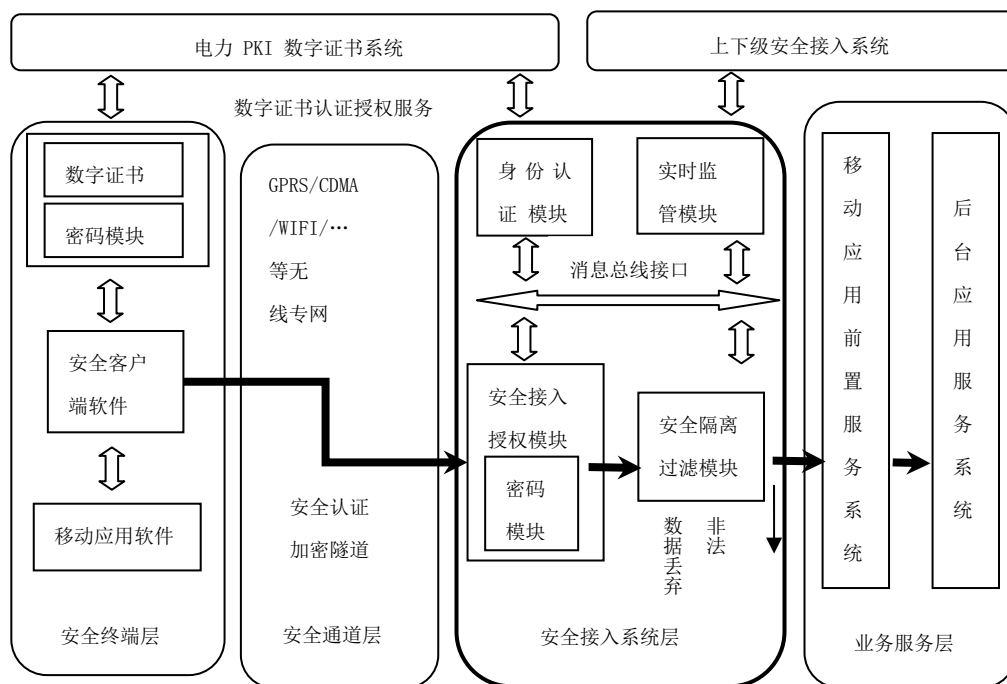


图1 系统逻辑结构设计

如图1所示，整个系统逻辑结构可分成安全终端层、安全通道层、安全接入系统层、业务服务层四个逻辑层次。安全终端层包括终端加密硬件、安全客户端软件及移动应用软件；安全通道层底层基于APN专线等构建无线专网，并在其上建立二次加密隧道进行数据保密传输；安全接入系统层是整个系统的核心部分，依托电力PKI数字证书系统，实现双向数字证书认证接入、授权与访问控制、安全隔离过滤、实时监控管理等重要功能，并通过消息总线进行各模块控制消息传递及协同配合，同时进行上下级安全接入系统间级联消息通讯。业务服务层主要包括移动应用前置服务系统、后台应用服务系统等，前者通过抽取、对外提供最小化的移动作业服务以进一步达到屏蔽越权及非法访问。

2.2 主要关键技术

2.2.1 组合式身份认证及安全接入技术

为实现对PDA终端的强身份认证，系统采取了数字证书认证结合终端特征识别及安全状态扫描为一体的组合身份认证机制。PDA终端采用闪存（SD）^[5]加密卡进行数字证书及密钥存储，SD加密卡是具有半导体快闪存储器及集成加密芯片的一种智能卡（SmartCard）^[6]。智能卡认证是双因子（2FA:Two-factor Authentication）^{[6][7]}认证的最普遍形式，认证安全性很高。

同时，为进一步增强安全性，防止一卡多用、黑客攻击等，系统在终端初始接入时，根据系统后台策略，随机收集终端硬件与证书信息、主机软硬件特征等，并通过哈希算法生成唯一的接入识别码，每次接入都会对终端进行接入识别验证。

通过数字证书进行双向高强度身份认证，在完成认证基础上进行密钥协商和后续数据加解密，在终端至主站系统之间，不依赖于运营商加密机制构建了一条高强度双向数据加密隧道，充分保证了数据传输的安全性。

2.2.2 安全客户端软件开发技术

PDA终端上的安全接入软件开发，重点需考虑Wince/Android/Symbian等移动操作系统兼容性，并适应原移动作业C/S模式双向通讯过程。在设计上主要采取了透明代理及转发技术、隧道复用技术等等，以保证和原有移动作业软件的无缝集成。

（1）透明代理及转发技术：系统采用了透明代理技术，通过透明监听报文、隧道连接保持、加密封装转发、数据解密、投递到指定业务系统等步骤进行客户端报文的透明转发，屏蔽了客户端应用和后台服务的差异，做到对移动应用、后台业务的无缝对接。

(2) 加密隧道复用设计技术：通常各主流厂商安全接入软件，针对 PDA 终端上的每一个业务应用都需和主站建立一条加密隧道，这样技术实现难度相对较小，但对系统整体处理能力要求较高，极易造成性能瓶颈。本系统采用了隧道复用技术，使每个 PDA 终端上的所有应用可复用同一条加密隧道，降低了系统负载，提高了并发处理能力，如图 2 所示。

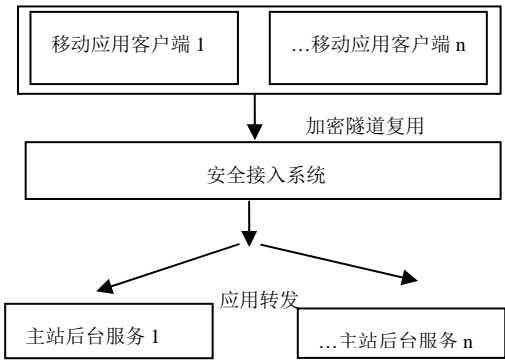


图 2 加密隧道复用设计

因此，针对不同客户端应用，结合不同的连接状态报文，需进行报文定义设计，并进行不同的状态处理，如图 3 所示。

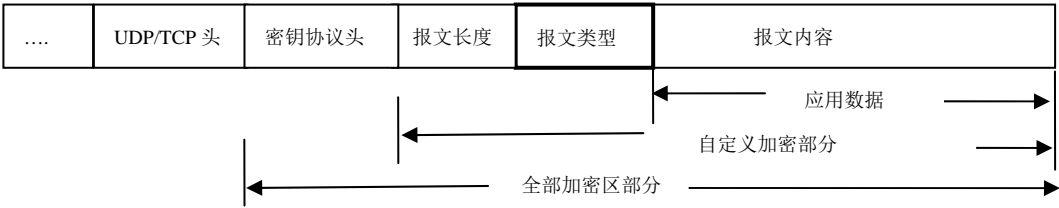


图 3 报文加密结构示意图

本系统共设计了二十余种报文类型，典型类型如连接请求、应答、断开，数据转发、扫描请求、认证返回、出错处理等，并可根据业务类型及安全需求进行动态扩展。

2.2.3 安全数据过滤技术

传统网闸等安全隔离技术通过双 CPU 处理单元进行网络隔离、TCP 层协议剥离与裸数据交换，但因处理性能、实现技术难度等很难实现对应用协议的安全过滤，或仅能支持简单的 URL 过滤等功能。本系统针对电力移动作业协议有限、可控特点，在传统隔离产品架构上进行了设计优化，在内、外网处理单元分别设计了交换层、调度层、插件层，如图 4 所示。

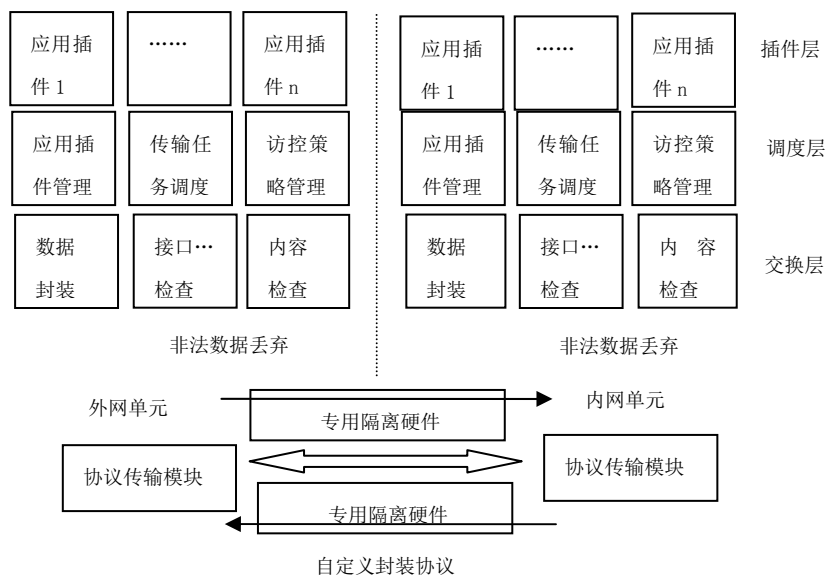


图4 安全隔离过滤模块设计图

(1) 交换层：分别实现自定义协议数据封装、接口及应用数据检查，依据应用插件层对协议接口格式、数据格式定义，过滤非法数据进行丢弃。

(2) 调度层：实现应用插件、传输任务、访问策略等的调度管理，并可根据业务重要程度动态调整任务优先级，同时可进行白、黑名单管理。同时可结合具体业务实际在安全性、传输效率间进行平衡，进行选择过滤。

(3) 插件层：根据电力应用协议类型动态扩展、加载应用插件，应用插件包括协议类型、数据格式等详细定义。

2.2.4 统一高速消息总线技术

传统安全防护体系中，各安全设备由不同厂商开发，只能各自完成单一功能，缺乏必要的协同工作能力。为此，系统基于面向服务的体系架构 SOA 思想，结合业务实际需求开发了统一高速消息总线接口，用于实现异构控制数据、应用数据的统一集成交换，第三方系统可通过 WEBSERVICE 描述语言 WSDL 等和系统进行接口集成及功能拓展。

系统各功能模块充当服务提供者、消费者双重角色。主要系统服务包括接入服务、访问服务、认证服务、策略服务、授权服务、加解密服务、代理服务、交换及过滤服务、监控服务、审计服务等等，并可动态扩展，通过统一的服务注册、发布、注销机制统一管理，并可进行内、外服务接口转换。

3 典型工程应用案例

目前，该系统已在全国部分网省公司、地市公司进行了试点应用，可广泛应用于电力生产、物资、营销、应急指挥、应急抢修等移动作业应用的安全防护，有力地保障了电力生产、管理业务的安全、稳定运行。

图5所示为某网省公司基于移动作业系统的接入拓扑结构图。

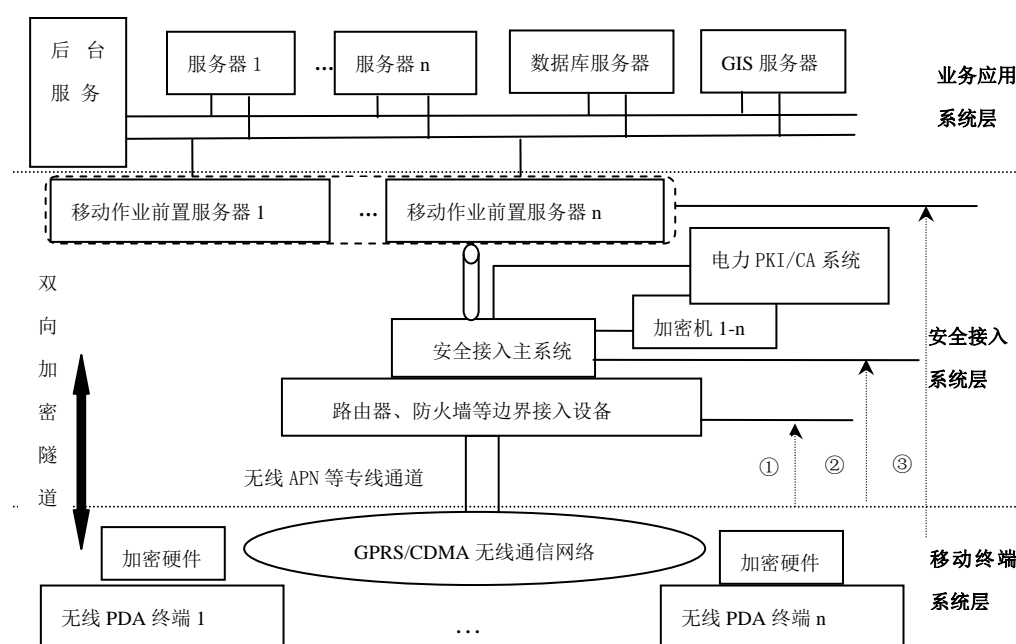


图 5 物理应用拓扑示意图

移动终端系统层包括支持加密硬件、无线通讯功能的 PDA 终端。安全接入系统层是整个系统的核心，主要完成安全认证与保密传输、安全隔离过滤、集中监控审计功能，逻辑上具有三层防护，如图 5 所示，分别为 APN 及边界防护、安全接入主系统防护、主站业务应用接口防护：

(1) 无线 APN 等专线通道、路由器及防火墙：第 1 层防护，如①所示，通过运营商提供的无线 APN 等专线通道、边界设备访问控制列表(ACL)控制、报文过滤策略设置等，禁止非法报文通过，并与 internet 公用信道隔离。

(2) 安全接入系统：第 2 层防护，如②所示，依托电力 PKI/CA^[8]系统与 PDA 终端进行数字证书双向认证、准入控制及细粒度访问控制等，建立双向加密隧道进行数据保密传输，同时进行内、外网安全隔离防护并进行数据安全过滤，以确保应用接口及数据安全。同时提供对终端安全接入策略、实时状态和操作行为的实时监控、安全审计等功能。安全接入系统的硬件设备采用嵌入式安全操作系统，具有强制访问控制 (MAC)^[9]等多种安全机制，可从底层确保操作系统安全。

(3) 移动应用前置系统：第 3 层防护，如③所示，为提高系统安全性，利用移动应用前置系统对外网终端访问业务进行逻辑抽取，只提供最小化移动作业服务接口，如查询、上传、下载接口等，防止终端越权访问。

(4) 业务应用系统层：包括生产、营销、应急、办公等后台服务系统等，通过移动应用前置系统提供最小化业务逻辑集合的移动作业对外接口服务。

经实际测试，实测非对称算法 1024bit 公钥运算 2000 次/s、私钥运算 800 次/s、对称算法运算在 PDA 终端侧可达 256.9kbps,网关侧可达 230Mbps，可同时并发接入 1500 终端，并可通过集群部署方式进行动态扩展，能基本满足移动作业接入业务的性能需求。

3 结束语

本文设计的电力移动作业 PDA 安全接入系统，针对电力传统移动作业 PDA 接入系统设计可能存在的安全问题，通过采用多种安全技术如双向数字证书认证与数据加密、透明转发、安全数据过滤、统一消息总线等等，进行了新的系统体系结构设计，较大地增强了电力移动作业应用的安全性及防护能力。该系统后续将在数据过滤效率及准确度、采用更高安全等级的加密算法、移动 PDA 终端自身安全防护、多种嵌入式移动终端接入支持等方面展开进一步深入研究工作。

参考文献：

- [1] 张金玲,黎峰,刘镇顶.基于PDA的移动作业标准化管理系统[J].计算机工程与设计,2008, 29(7):1831-1832.
- [2] 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].电力系统及其自动化,2003, 27 (24):63-65.
- [3] 3G GSM密码遭破解[EB/OL]. <http://it.solidot.org/article.pl?sid=10/01/15/0536242>.
- [4] 屈波,熊前兴,吴业福,等.基于物理隔离的安全网闸研究与系统设计[J].计算机科学,2004, 31 (Z1):222-225.
- [5] SD密码卡解决方案:移动安全新篇章[EB/OL].<http://www.bokee.net>.
- [6] 李祥.智能卡研发技术与工程实践[M].北京:人民邮电出版社,2003.
- [7] 杨修兰,蒋泽军,王丽芳.基于LDAP和双因素身份认证的统一认证[J].计算机工程与科学,2008,30(7):27-29,39.
- [8] 段斌,刘念,王健,等.基于PKI/PMI的变电站自动化系统访问安全管理[J].电力系统自动化,2005,29(23):58-63.
- [9] 刘威鹏,胡俊,吕辉军,等.LSM框架下可执行程序的强制访问控制机制[J].计算机工程,2008, 34(7):160-162.

作者简介：

秦超(1978—)，男，硕士，工程师，从事电力系统信息网络安全的研究及开发；

张涛(1976—)，男，硕士，高级工程师，从事电力系统信息网络安全的研究及开发；

林为民(1964—)，男，硕士，研究员级高级工程师，从事电力系统信息网络安全的研究及管理。