DOI: 10.3969/j.issn.1000-1026.2012.11.015

电力移动作业 PDA 安全接入系统设计与实现

秦 超[1,2], 张 涛[1,2], 林为民[1,2]
(1. 国网电力科学研究院/南京南瑞集团公司, 江苏省南京市 210003; 2. 中国电力科学研究院, 北京市 100192)

摘要: 分析了传统电力移动作业个人数字助理(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: 信息网络安全; 电力移动作业; 个人数字助理; 安全接入系统; 安全数码加密卡; 公钥基础设施; 双因子认证; 安全隔离过滤

0 引言

目前,电力系统已逐渐采用个人数字助理(PDA)[1]通过通用分组无线电业务/码分多址(GPRS/CDMA)公共网络接入电力生产、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和接入流程设计,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 网络由专线接入点(access point name, 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。其主要安全隐患如下。

1)身份认证强度低。手机号绑定特定 APN 网络,经 GPRS 网关支持节点(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 服务支持节点(SGSN)[2]→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和数据过滤[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)终端集中监管和访问控制困难。各移动作业子系统相互独立,信息无法重用,难以进行精细监控和管理,维护成本高,易造成安全隐患。

5)终端行为安全审计困难。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和细粒度地进行安全审计。

2 电力移动作业 PDA 安全接入系统设计

为了解决上述安全问题,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。

2.1 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 4 个逻辑层次。

安全终端层包括终端加密硬件、安全客户端软件和移动应用软件。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,依托电力公共密钥基础结构(PKI)数字证书系统,实现双向数字证书认证接入、授权和访问控制、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和协同配合,同时进行上下级安全接入系统间级联消息通信。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和非法访问。

收稿日期: 2011-04-22; 修回日期: 2011-11-29。

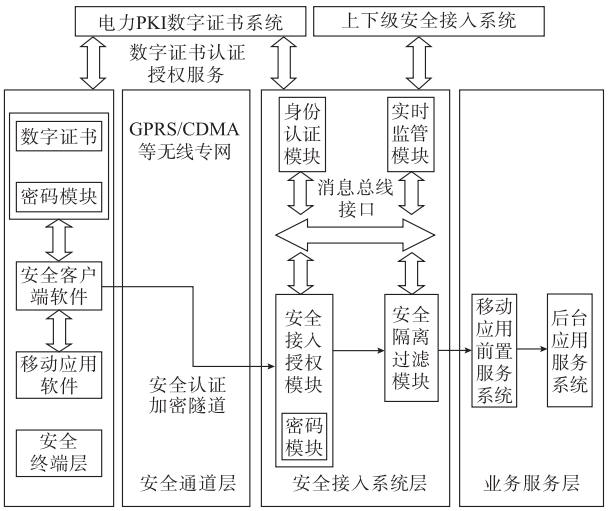

图 1 系统逻辑结构设计
Fig. 1 Logical structure design of system

2.2 主要关键技术

2.2.1 组合式身份认证和安全接入技术

为了实现对 PDA 终端的强身份认证,系统采取集数字证书认证结合终端特征识别和安全状态扫描于一体的组合身份认证机制。PDA 终端采用加密的安全数码存储卡(即 SD 卡)[5]进行数字证书及密钥存储,SD 卡是具有半导体快闪存储器和集成加密芯片的一种智能卡[6]。智能卡认证是双因子(two-factor authentication,2FA)[6-7]认证的最普遍形式,认证安全性很高。

同时,为了进一步增强安全性,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,随机收集终端硬件和证书信息、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,并适应原移动作业客户/服务器(C/S)模式双向通信过程。在设计上,主要采取透明代理和转发、隧道复用等技术,以保证与原有移动作业软件的无缝集成。

采用透明代理技术,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,屏蔽了客户端应用与后台服务的差异,做到对移动应用、后台业务的无缝对接。

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与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。

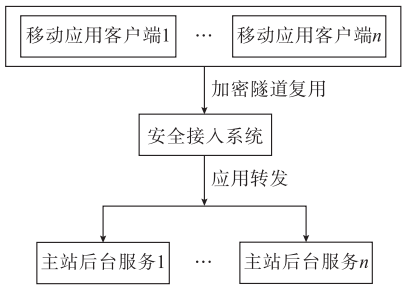

图 2 加密隧道复用设计
Fig. 2 Design of reuse encrypted tunnel

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。图中,UDP 为用户数据报协议,TCP 为传输控制协议。

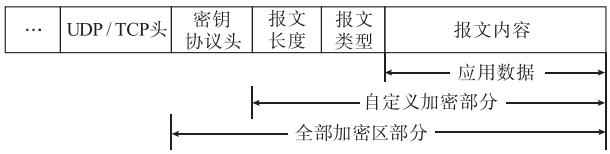

图 3 报文加密结构示意图
Fig. 3 Encryption structure schematic diagram of packet

本系统设计了 20 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,并可根据业务类型和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中央处理器(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,或仅能支持简单的统一资源定位符(URL)过滤等功能。本系统针对电力移动作业协议有限、可控的特点,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。

交换层分别实现自定义协议数据封装、接口和应用数据检查,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。

调度层实现应用插件、传输任务、访控策略等的调度管理,可根据业务重要程度动态调整任务优先

级，并可进行白、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，进行选择性过滤。

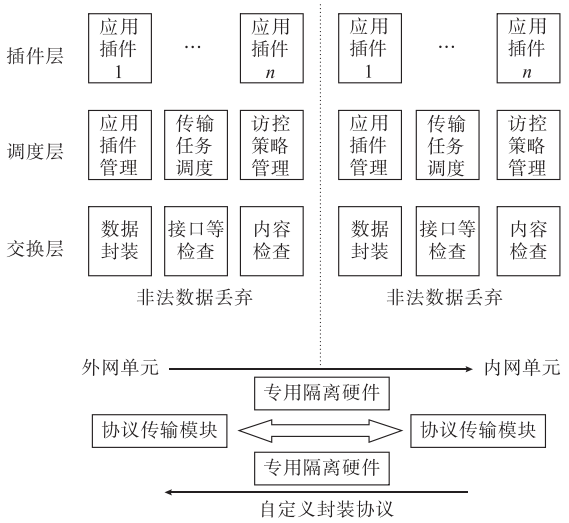

图 4　安全隔离过滤模块设计
Fig. 4　Design of securely gapping and filtering module

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 Web 服务描述语言(WSDL)等与系统进行接口集成和功能拓展。

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、访控服务、认证服务、策略服务、授权服务、加解密服务、代理服务、交换和过滤服务、监控服务、审计服务等，可动态扩展，通过统一的服务注册、发布、注销机制进行统一管理，并可进行内、外服务接口转换。

3　典型工程应用案例

目前，该系统已在国内部分网省公司、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、管理业务的安全和稳定运行。

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。

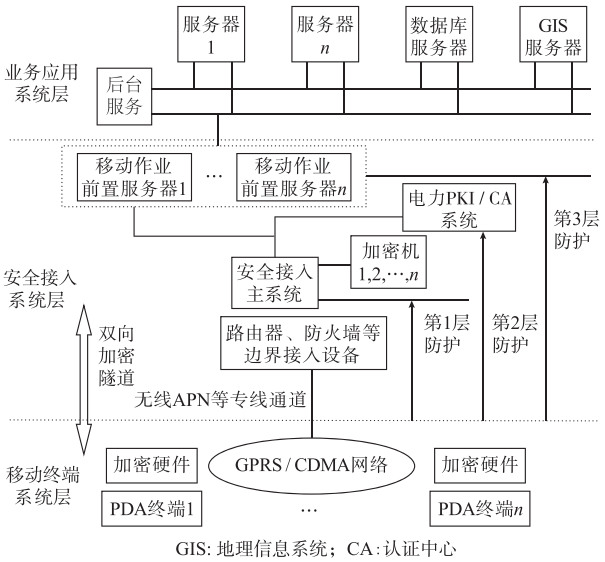

图 5　物理应用拓扑示意图
Fig. 5　Topology diagram of physical application

移动终端系统层包括支持加密硬件、无线通信功能的 PDA 终端。

安全接入系统层是整个系统的核心，主要完成安全认证和保密传输、安全隔离过滤、集中监控审计功能，逻辑上具有以下 3 层防护。

1)第 1 层防护：无线 APN 等专线通道、路由器和防火墙。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，并与因特网公用信道隔离。

2)第 2 层防护：安全接入系统。依托电力 PKI/CA[8]系统和 PDA 终端进行数字证书双向认证、准入控制和细粒度访问控制等，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，以确保应用接口和数据的安全。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，具有强制媒体访问控制(MAC)[9]等多种安全机制，可从底层确保操作系统安全。

3)第 3 层防护：移动应用前置系统。为了提高系统的安全性，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。

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 1 024 bit 公钥运

算 2 000 次/s,私钥运算 800 次/s,对称算法运算在 PDA 终端侧可达到 256.9 kbit/s,网关侧可达到 230 Mbit/s,可同时并发接入 1 500 个终端,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。

4 结语

本文所述的电力移动作业 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和数据加密、透明转发、安全数据过滤、统一消息总线等,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和防护能力。该系统后续将在数据过滤效率和准确度、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进一步展开深入的研究工作。

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):1831-1833.
ZHANG Jinling, LI Feng, LIU Zhending. Standard management system of mobile operation based on PDA[J]. Computer Engineering and Design, 2008, 29(7): 1831-1833.

[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]. 电力系统自动化,2003,27(24):63-64.
LI Huiyu, LUO Xiaoli, YU Shenglin. A GPRS based distribution automation system [J]. Automation of Electric Power Systems, 2003, 27(24): 63-64.

[3] 3G GSM 密码遭破解[EB/OL]. [2010-01-15]. 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(B9):222-226.
QU Bo, XIONG Qianxing, WU Yefu, et al. Study of security network gap based on physics solation[J]. Computer Science, 2004, 31(B9): 222-226.

[5] SD密码卡解决方案:移动安全新篇章[EB/OL]. [2010-10-29]. 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 和双因子身份认证的统一认证[J]. 计算机工程与科学,2008,30(7):27-29.
YANG Xiulan, JIANG Zejun, WANG Lifang. Unified authentication based on LDAP and double-factor authentication [J]. Computer Engineering and Science, 2008, 30(7): 27-29.

[8] 段斌,刘念,王键,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.
DUAN Bin, LIU Nian, WANG Jian, et al. Access security of substation automation systems based on PKI/PMI [J]. Automation of Electric Power Systems, 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.
LIU Weipeng, HU Jun, LÜ Huijun, et al. Mandatory access control mechanism of executable program under LSM [J]. Computer Engineering, 2008, 34(7): 160-162.

秦 超(1978—),男,通信作者,硕士,工程师,主要研究方向:电力系统信息网络安全。E-mail: qinchao@epri.sgcc.com.cn

张 涛(1976—),男,硕士,高级工程师,主要研究方向:电力系统信息网络安全。E-mail: zhangtao@epri.sgcc.com.cn

林为民(1964—),男,硕士,研究员级高级工程师,主要研究方向:电力系统信息网络安全。E-mail: linweimin@epri.sgcc.com.cn

Design and Implementation of Safe Access System for Electric Mobile Operation Based on PDA

QIN Chao[1,2], *ZHANG Tao*[1,2], *LIN Weimin*[1,2]

(1. State Grid Electric Power Research Institute, Nanjing 210003, China;
2. China Electric Power Research Institute, Beijing 100192, China)

Abstract: An in-depth analysis is made of the possible hidden risks to the traditional access system for electric power mobile operation based on the personal digital assistant (PDA). A safer access system for electric power mobile operation based on PDA is then designed and implemented, with its architecture and components thoroughly analyzed. Capable of such functions as certificate verification of both the PDA and the safe access system, data transmission security, safe access control, network separating and data filtering, real-time monitoring and audit, etc, this system can effectively promote the security and protection of electric power mobile operation.

Key words: information network security; electric power mobile operation; personal digital assistant (PDA); safe access system; secure digital encryption card; public key infrastructure; dual factor authentication; safe separation and filter