



国网客服中心南北园区无线 VPN 组网结构及安全防护

邹颖, 王一蓉, 王艳茹, 王思宁

(北京国电通网络技术有限公司, 北京 100070)

摘要:探索了适用于国家电网客服中心南北园区的无线虚拟专网组网结构,该结构将充分考虑园区的无线应用和通信需求。分析了无线虚拟专网存在的安全接入风险和无法管控的缺陷,并提出了适用于园区的解决思路;从终端、网络、边界和应用 4 个层面深入研究无线虚拟专网在园区组网的安全性,可以为园区无线虚拟专网的设计和建设提供参考。

关键词:无线虚拟专网;业务承载;组网结构;安全防护

中图分类号: TN915.853

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016075

Wireless VPN network structure and safety protection in the north and south call center of SGCC

ZOU Ying, WANG Yirong, WANG Yanru, WANG Sining

Beijing GuoDianTong Network Technology Co., Ltd., Beijing 100070, China

Abstract: The wireless virtual private network structure suitable for the north and south call center of SGCC was explored. In the structure, the wireless applications and communication of the north and south call center of SGCC were considered. The existing access security risks and the cannot-control defects of wireless virtual private network were analyzed, and the solutions for the center were given. Through the research on wireless virtual private network security from the four aspects as the terminal, network, boundary and application, reference for the design and construction of the center wireless virtual private network was provided.

Key words: wireless virtual private network, service bearer, network structure, safety protection

1 引言

根据国家电网公司(State Grid Corporation of China, SGCC)客服中心南北园区“安全性、创新性、经济性、开放性”的园区体系设计,全面整合园区分布式能源,广泛集成能量信息,实现对多种能源的协调控制和综合能效管理;建成多点接入、网络共享、需求感知的园区能源互联网,以人为本、以创新为驱动,通过丰富专业的服务和业务,服务

园区的运营、办公和生活;物联网、云服务、大数据等智慧元素的融入,实现了各类服务的高度集成和相互联动,凸显了“安全高效、智能互动、绿色健康、舒适便捷”的智慧特征。无线虚拟专网作为重要的无线网络边缘接入手段,将在一定程度上丰富和完善南北园区的无线通信需求。

本文从无线虚拟专网的组网架构及安全防护 2 个主要方面入手,为园区无线网络边缘接入的规划、设计和建设提供参考。



2 需求分析

2.1 业务承载需求

园区无线虚拟专网的基础功能是满足园区无线应用业务现状和未来新增无线业务的接入需求,是保证园区无线虚拟专网在新形势下的扩展和支撑园区物联网发展的重要基础网络,可在促进电网生产运行和企业管理全过程的全景感知、信息融合及智能管理与决策方面发挥重要作用。智能电网无线应用业务需求分为智能电网广泛采集类、业务互动化类、数据实时处理类、识别与定位类、远程控制类和监控告警类等^[1,2]。

作为园区通信的补充手段,园区无线虚拟专网的应用能进一步提升园区传感器网络覆盖、管理数据采集、决策信息化支持以及数据类别数量采集的质量和效率。

2.2 网络需求

国家电网公司在“十二五”通信网规划中提出,“十二五”期间坚强智能电网建设不仅要求通信网在核心层要有强大的承载能力和坚强网络架构,还要在接入层有广泛、灵活的边缘接入能力^[3,4]。

在将园区信息互联互通的程度以及园区内接入网络的及时性和便捷程度作为园区信息通信主要考核指标的基础上,园区对通信网接入能力提出了全方位、多样化、灵活便利、经济高效等要求。园区无线应用业务的多样性对承载无线应用的无线虚拟专网在接入质量和速率、传输质

量和速率、提供的服务以及管理方面提出了更高的要求。

2.3 安全防护需求

园区无线虚拟专网的安全防护应积极采用各种先进技术,在接入安全、通道安全、边界安全、安全审计等方面加以防范,确保无线应用数据传输的安全性。园区无线虚拟专网安全防护应做到“事前预防、事中监督、事后处理”,管理手段与技术措施相结合,保障园区无线虚拟专网及其所承载业务的安全稳定运行。

3 组网结构设计

根据国家电网客服中心南北园区的地域特点和业务需求以及园区无线应用业务分散接入等问题,宜建设集中接入的园区无线虚拟专网^[5,6]。

3.1 网络架构

园区无线虚拟专网的网络位置示意如图1所示。

园区无线虚拟专网总体组网架构采用各园区分别与当地运营商进行专线对接的模式,园区无线虚拟专网架构如图2所示。

对于需要接入信息内网的业务,业务数据从终端接入运营商的无线网络,使用运营商的不同隧道技术进行封装,经过虚拟专属通道传输至目的地址进行解封装,还原业务数据格式后,通过专线接入信息内网。若该业务需汇聚至国家电网公司总部,业务数据将通过综合数据网从各园区信息内网传输至公司总部信息内网。该组网方式在实

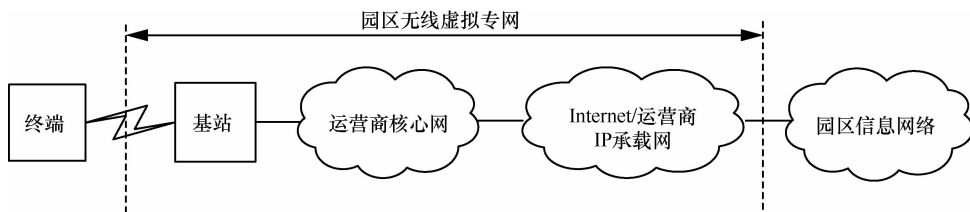


图1 园区无线虚拟专网的网络位置示意

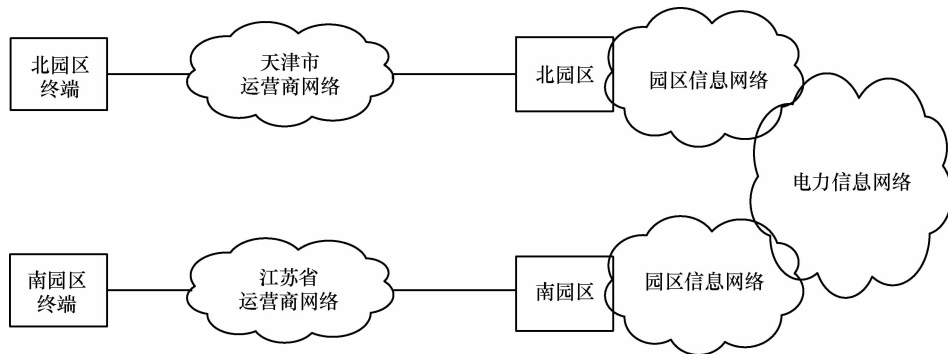


图2 园区无线虚拟专网架构

现园区对网络出口的统一管理、提高出口资源利用率的同时,避免了因分散接入造成的资源浪费以及因分散建设和管理产生的安全隐患。

3.2 网络接入方案

园区无线虚拟专网业务终端依托运营商网络接入,可采用 APN 接入或 VPDN 拨号接入方式。

3.2.1 APN 接入

APN 接入方式适用于对安全性要求不高的业务终端的接入,基本要求如下:

- 业务终端应采用园区专用 APN 接入;
- APN 使用原则建议按照业务的安全等级进行分类,不同安全等级的业务使用不同的 APN 接入;
- 应支持 IP 地址静态分配和动态分配。

3.2.2 VPDN 拨号接入

VPDN 拨号接入方式适用于对安全性要求较高的业务终端的接入,基本要求如下:

- VPDN 拨号接入应采用 L2TP 隧道技术;
- 各园区应纳入各对应省市电力公司的自建 LNS 及 AAA 服务器范畴中;
- 应支持 IP 地址静态分配和动态分配。

3.3 网络传输方案

园区无线虚拟专网业务数据在运营商承载网中传输可采用 GRE 隧道技术或 L2TP 隧道技术。

3.3.1 GRE 隧道传输技术

GRE 方式^[7]在网络接入时不进行用户名和密码的认证,安全性偏低,需要在业务层进行安全控制,这种接入方式部署简单、灵活,适合业务终端量较大且对安全性要求不高的

无线应用,目前中国移动和中国联通均支持此方式。

业务终端采用专用 APN 接入时,业务数据从运营商核心网的网关支持节点到园区信息网络边界传输时,使用 GRE 隧道技术,GRE 隧道可选择终结于运营商侧或园区侧:GRE 隧道终结于园区侧时,其终结于园区边界示意如图 3 所示;GRE 隧道终结于运营商侧时,运营商网关支持节点到运营商边界设备宜使用 GRE 或 GRE+MPLS-VPN 隧道技术,GRE 隧道终结于运营商边界示意如图 4 所示。

3.3.2 L2TP 隧道传输技术

对于安全级别要求高的无线应用,建议使用 L2TP 方式^[8]。业务终端采用 VPDN 拨号接入时,业务数据从运营商核心网的网关支持节点到园区信息网络边界传输宜使用 L2TP 隧道技术,应纳入相应省市电力公司 LNS。

纳入省市电力公司自建 LNS 时,从运营商网关支持节点到电力 LNS 采用 L2TP 隧道传输,L2TP 隧道示意如图 5 所示。

租用运营商 LNS 时,从运营商网关支持节点到运营商 LNS 采用 L2TP 隧道传输,运营商 LNS 到运营商边界设备采用 MPLS-VPN 隧道或专线传输,L2TP+MPLS-VPN 隧道示意如图 6 所示,L2TP 隧道示意如图 7 所示。

3.4 网络边界部署

(1) 边界部署方式 1

网络边界部署方式 1 适用于以下 2 种情况:业务终端采用专用 APN 接入;业务终端采用 VPDN 拨号接入,租用运营商的 LNS 及 AAA 服务器。各园区宜在网络边界部署园区边界接入设备、边界防护设备和入侵检测设备,其中

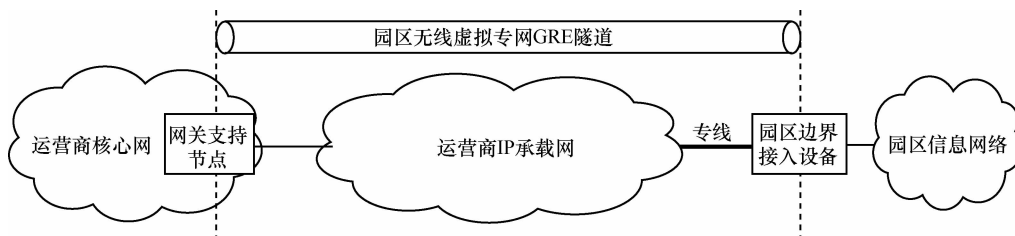


图 3 GRE 隧道终结于园区边界示意

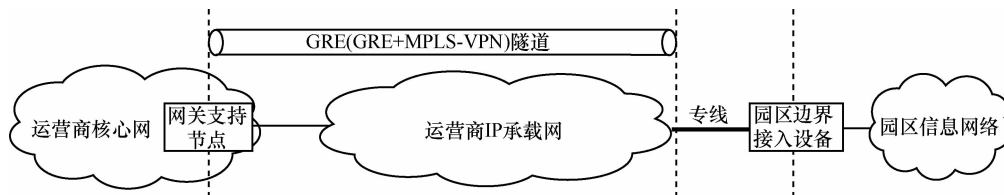


图 4 GRE 隧道终结于运营商边界示意



图5 L2TP隧道示意(相应省市电力公司自建LNS)



图6 L2TP+MPLS-VPN隧道示意(租用运营商LNS)

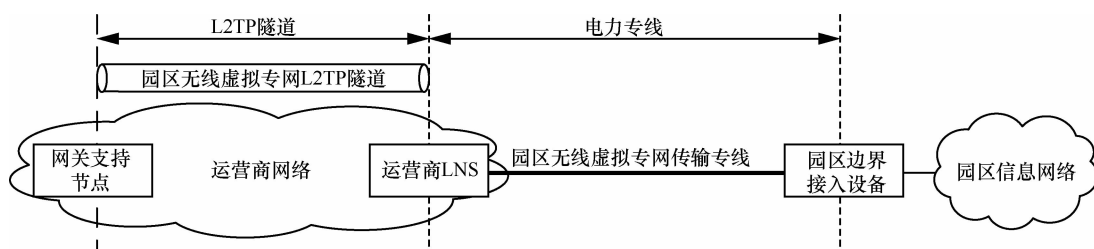


图7 L2TP隧道示意(租用运营商LNS)

园区边界接入设备和边界防护设备宜采用冗余热备份的方式部署。网络边界部署方式1如图8所示。

(2) 边界部署方式2

网络边界部署方式2适用于业务终端采用VPDN拨号接入,该方式下的LNS和AAA服务器可利用各相应省市电力公司自建的LNS及AAA服务器。各园区网络边界宜部署电力LNS设备、AAA服务器、边界防护设备和入侵检测设备,其中LNS设备和边界防护设备宜采用冗余热备份的方式部署。网络边界部署方式2如图9所示。

3.5 可靠性设计

(1) 网络链路

运营商应提供园区无线虚拟专网骨干传输链路的冗余保护技术;各园区与各运营商互联的专线应有物理不同路由的冗余保护线路;园区无线虚拟专网边界设备互联应有冗余保护线路。

(2) 网络核心设备

园区无线虚拟专网核心设备边界接入设备、边界安全防护设备等宜采用冗余热备份的方式组网,不具

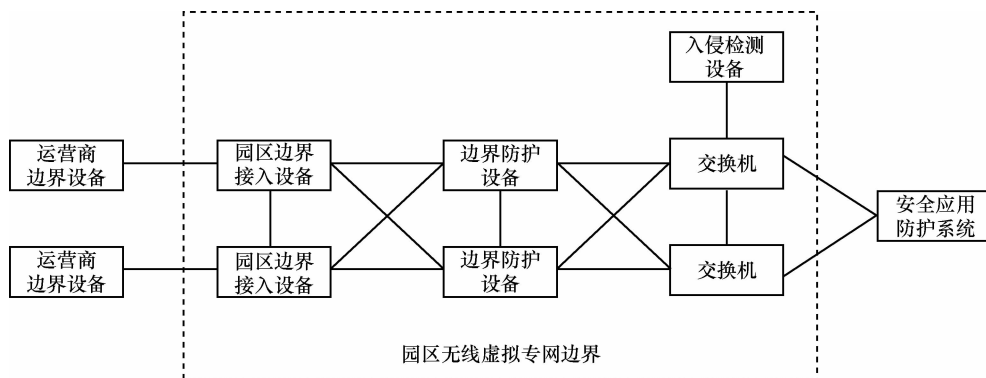


图8 网络边界部署方式1

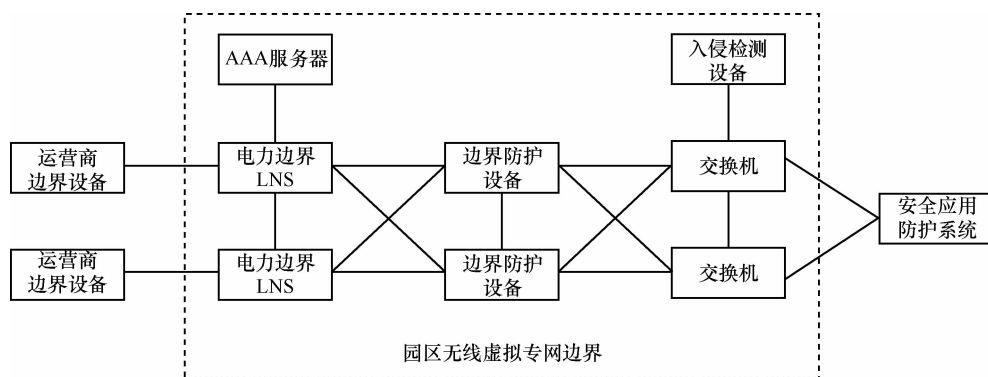


图9 网络边界部署方式2

备份冗余热备份条件的可采用冗余冷备份的方式组网。

4 安全防护研究

园区无线虚拟专网的安全防护应在接入安全、通道安全、边界安全、安全审计等方面加以防范^[9]。如采用加密技术、接入认证技术、冗余备份技术、访问控制技术、安全审计技术、网络管理技术等,为园区无线虚拟专网提供数据加密、身份认证、安全备份、访问控制、安全审计、数据完整性验证等多种安全防护保障,有效抵抗窃取网络信息、篡改网络数据和网络重放攻击,确保园区无线虚拟专网数据的机密性,保证其数据的安全性。在园区无线虚拟专网日常运行维护管理中,应加强规范管理,严格执行安全运行维护等管理制度,建立相应的应急响应体系。

4.1 接入安全

终端接入园区信息网络时,采用AAA认证技术进行接入控制,验证终端的合法性(如验证终端的用户名、密码、IMSI等信息)。同时,根据接入终端类型的不同采用不同的策略,生产类终端要求运营商支持APN/VPDN接入点与SIM卡绑定,一张SIM卡只允许一个APN/VPDN接入,

非生产类终端采用数字证书的方式进行接入认证。

4.2 通道安全

园区无线虚拟专网传输通道包括运营商通道和边界接入通道两部分,其中运营商通道又可分为无线接入通道与有线传输通道。园区无线虚拟专网通道示意如图10所示。

4.2.1 运营商通道

无线接入通道是指从终端至无线基站的无线通信链路,有线传输通道是指从无线基站至运营商网络边界的通信链路。运营商通道具备良好的冗余性,能确保业务不受通道故障的影响;无线传输通道应进行加密,以防止非法窃听;无线基站应提供一定的接入能力,以防止通信通道被占用而导致终端无法进行数据传送;有线传输通道应支持L2TP/GRE隧道技术,建立电力专属虚拟链路,结合IPSec等加密技术措施,确保虚拟专属通道的私有性与安全性。

4.2.2 边界接入通道

边界接入通道是指从运营商有线网络边界至园区信息网络边界的通信链路。边界接入通道采用专用链路,使用双物理链路提供链路的冗余,采用专用加密通道技术保证边界接入链路传输的安全性。

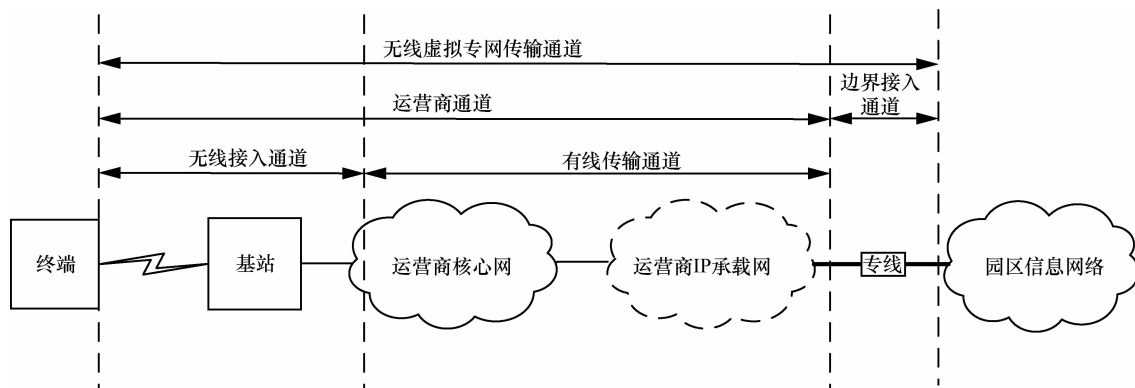


图10 园区无线虚拟专网通道示意



4.3 边界安全

在园区无线虚拟专网网络边界建立一套多层次的全面安全防护体系,包含边界防护设备与安全应用防护系统。边界防护设备功能包括访问控制、入侵检测、数据过滤;安全应用防护系统应具备安全隔离、完整性校验等业务应用安全防护功能。网络边界安全防护体系逻辑架构如图 11 所示。

4.3.1 边界防护设备

边界防护设备应满足《信息系统安全等级保护基本要求》的要求,边界防护设备具有以下防护功能。

- 访问控制。边界防护设备具有访问控制功能,访问控制通过对数据分组的源地址、目的地址、源端口、目的端口、网络协议等参数进行配置,对进出信息网络的数据流制定细粒度访问控制策略。
- 入侵检测。边界防护设备具备入侵检测功能,入侵检测功能可以检测网络中 3~7 层的入侵行为,并进行告警。
- 数据过滤。边界防护设备宜具备对接入的数据报文进行分析与校验的功能,保障接入数据的安全性。

4.3.2 安全应用防护系统

与园区信息网络进行数据交互的业务宜采用安全应用防护系统提供安全隔离、完整性校验等应用安全服务,对安全应用防护系统的基本要求如下:

- 支持对终端进行软、硬件信息的完整性校验;
- 支持信息网络与终端之间的双向隔离以及安全数据交换,任何形式的数据分组、信息传输命令和

TCP/IP 都无法穿透。

4.3.3 安全审计

安全审计应满足《信息系统安全等级保护基本要求》与《电力二次系统安全防护总体方案》的要求。安全审计由一级安全审计系统、二级安全审计系统和安全审计探针组成。安全审计防护逻辑示意如图 12 所示。

一级安全审计系统基本要求如下:支持与二级安全审计平台之间通过专有的协议进行安全数据交换;能存储 6 个月内各园区公司二级安全审计平台上报的各类安全事件;能实时展现各园区二级安全审计平台上报的高级安全事件。

二级安全审计系统基本要求如下:支持与一级安全审计平台以及安全审计探针之间通过专有的协议进行安全数据交换;能接收并分析安全审计探针上报的流量信息,建立正常业务需求的最小访问关系系统模型;能通过最小访问关系模型对流量信息进行实时监控,检出业务系统中有超出模型制定的流量,即判定为异常网络行为;判断并展现网络异常行为,如违反通信协议的异常网络流量、内部人员的非授权访问和恶意攻击、通过内部主机作为跳板的非授权访问、内部的恶意程序传播。

安全审计探针基本要求如下:支持与二级安全审计平台之间通过专有的协议进行安全数据交换;部署于 GRE、L2TP 隧道解封封装终结点之后的数据交换装置处;支持基于业务协议的实时安全审计,能识别终端与应用系统之间的应用协议,能检测协议误用,能检测 DDoS、蠕虫、病毒、木马等常见网络威胁;支持流量特征采集并上送到二级安

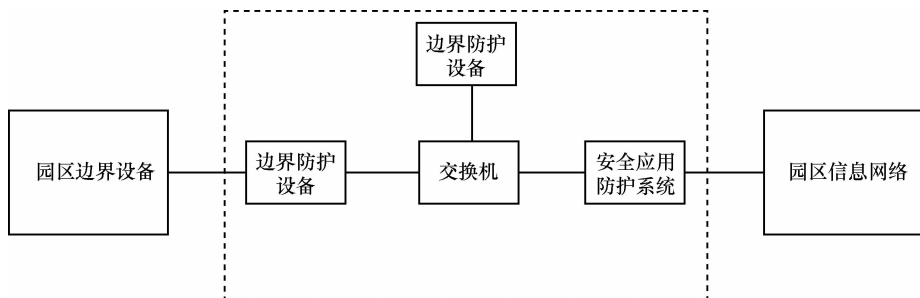


图 11 网络边界安全防护体系逻辑架构

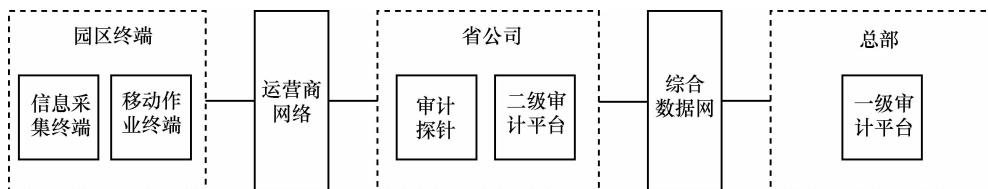


图 12 安全审计防护逻辑示意

全审计平台,包含来源IP地址、来源端口号、目的IP地址、目的端口号、协议种类、服务种类等特征字段。

4.4 管理安全

建立园区无线虚拟专网的运行维护安全制度与相应的应急响应联动机制,并满足国家电网公司与国家的安全要求。建立无线虚拟专网的终端安全管理、人员安全管理、SIM卡安全管理、运行值班安全管理等安全管理制度。

5 结束语

国家电网公司客服中心南北园区无线虚拟专网是在充分考虑国家电网公司信息通信网络资源的基础上,借助于移动运营商的2G/3G/4G无线接入网络,通过无缝的网络衔接和成熟的技术融合,打造了一个端到端的、系统化的、规范化的、可管可控的园区无线虚拟专网,提供安全、专用的信息传输通道,并研发了一个融合语音、短信、数据、图像、视频等多业务和应用的、可扩展的智能管控系统,实现对园区无线通信业务的有效补充和稳步推进,支撑园区物联网的发展,促进园区生产运行及管理的全过程信息融合、全景全息感知及智能管理与决策^[10]。同时将园区无线虚拟专网统一纳入国家电网公司园区无线虚拟专网管理平台,并单独为国家电网公司客服中心南北园区划分独立的平台管理域。

参考文献:

- [1] 孔震,叶文宸. 移动应用技术在坚强智能电网中的作用[N]. 国家电网报, 2012-05-22.
KONG Z, YE W C. The role of mobile application technology in the smart grid[N]. State Grid News, 2012-05-22.
- [2] ARAVINTHAN V, KARIMI B. Wireless communication for smart grid applications at distribution level-feasibility and requirements [C]//Power and Energy Society General Meeting, July 24-29, 2011, San Diego, CA, USA. New Jersey: IEEE Press, 2011: 1-8.
- [3] PATEL A, APARICIO J, TAS N, et al. Assessing communications technology options for smart grid applications [C]//2011 IEEE International Conference on Smart Grid Communications, October 17-20, 2011, Brussels, Belgium. New Jersey: IEEE Press, 2011: 126-131.
- [4] 徐益强. 基于3G的无线VPDN业务网的设计与实现[J]. 环境预警与监控, 2010, 2(5): 27-30.
XU Y Q. Design and implementation of 3G-based wireless VPDN business network [J]. Environmental Monitoring and Forewarning, 2010, 2(5): 27-30.

- [5] 王一蓉, 邹颖, 王艳茹. 电力无线虚拟专网组网架构及IP地址分配研究[J]. 电力信息与通信技术, 2014, 12(6): 16-21.
WANG Y R, ZOU Y, WANG Y R. Study of network architecture and IP address allocation of wireless VPN for power grid [J]. Electric Power Information and Communication Technology, 2014, 12(6): 16-21.
- [6] ZOU Y, WANG Y R, WANG N. Study of network architecture and IP address allocation of wireless VPN for power grid [J]. Electric Power Information and Communication Technology, 2014(6): 305-309.
- [7] HANKS S, LI T, FARINACCI D, et al. RFC 1702-generic routing encapsulation over IPv4 networks[Z/OL]. [2015-09-20]. http://xueshu.baidu.com/s?wd=paperuri%3A%283ba92bb792333f374e6c45a78f9d6aae%29&filter=sc_long_sign&tn=SE_xueshusource_2kduw22v&sc_vurl=http%3A%2F%2Fcitepeer.ist.psu.edu%2Fviewdoc%2Fsummary%3Fdoi%3D10.1.1.375.9348&ie=utf-8.
- [8] TOWNSLEY W, VALENCIA A, RUBENS A, et al. RFC2661-layer two tunneling protocol 'L2TP' [Z/OL]. [2015-09-20]. <http://www.faqs.org/rfcs/rfc2661.html>.
- [9] PI J Y, LIU X S, LIAO D Y, et al. A security scheme for power dispatching data network based on VPN[J]. Automation of Electric Power Systems, 2007, 31(14): 94-97.
- [10] 王一蓉, 佟大力, 邓伟. 电力无线虚拟专网应用分析及网络设计[J]. 电力信息与通信技术, 2013, 11(12): 49-52.
WANG Y R, TONG D L, DENG W. Application analysis and network design of power grid wireless VPN [J]. Electric Power Information and Communication Technology, 2013, 11(12): 49-52.

[作者简介]



邹颖(1978-),男,北京国电通网络技术有限公司工程师,主要研究方向为电力信息通信网络、无线通信和信息安全。

王一蓉(1979-),女,北京国电通网络技术有限公司高级工程师,主要研究方向为电力信息通信网络、无线通信和电力光纤到户。

王艳茹(1985-),女,北京国电通网络技术有限公司工程师,主要研究方向为电力信息通信、信息安全。

王思宁(1978-),女,北京国电通网络技术有限公司工程师,主要研究方向为电力信息通信网络、无线通信、电力光纤到户。