



电力 4G 无线通信网络安全技术

李坚¹, 刘昀², 安春燕³, 任建伟²

(1. 国网冀北电力有限公司, 北京 100053;

2. 国网冀北电力有限公司信息通信分公司, 北京 100053;

3. 全球能源互联网研究院, 北京 102209)

摘要: 4G 无线通信具有技术体制成熟、速率高、灵活等优点, 在电力配电自动化系统中具有广阔的应用前景。但电力通信对网络安全要求高, 电力 4G 网络的安全防护体系尚不成熟。针对电力 4G 网络应用模式, 分析了电力 4G 网络的安全风险, 最后针对安全风险提出了具体的安全防护策略和措施, 为 4G 网络在电力系统中的推广应用提供了指导。

关键词: 电力 4G; 安全风险; 安全防护

中图分类号: TN918.91

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2015384

Security technologies in 4G network for power grid

LI Jian¹, LIU Yun², AN Chunyan³, REN Jianwei²

1. State Grid Jibei Electric Power Company, Beijing 100053, China

2. State Grid Jibei Information and Communication Company, Beijing 100053, China

3. Global Energy Interconnection Research Institute, Beijing 102209, China

Abstract: 4G technologies with high data rate is flexible and has matured sufficiently, it has a promising application prospect in automatic distribution systems. However, communication networks for power grid should be more security, but the security protection of 4G network for power grid is not mature. Based on the application mode of 4G network in power system, the security risk was analyzed, then the specific safety protection methods were presented, which would guide the further application of 4G network in power system.

Key words: 4G network for power grid, security risk, security protection

1 引言

电力通信是支撑配电自动化建设、保障配电安全性和可靠性的重要技术之一。无线通信技术具有灵活、覆盖率高、无需铺设线路、成本低廉等优点, 在电力通信中占据重

要的位置。例如, 10 kV 通信接入网中, B、C 类区域以无线通信技术为辅, D、E 类通信区域以无线通信技术为主。而我国大部分区域为 B、C、D、E 类区域, 配电自动化建设落后。4G 通信技术^[1]作为无线公网中最成熟的新技术, 速率高、容量大且已进入大规模的商用阶段, 具有广阔的应用前景。

收稿日期: 2015-11-01; 修回日期: 2015-12-11

基金项目: 国家电网公司科技项目“电力复杂电磁环境下高可靠短距离无线通信关键技术研究”(No. SGRIXTKJ[2015]796)

Foundation Item: The Science and Technology Project of State Grid Corporation of China “Research on Key Technologies of High Reliability and Short Distance Wireless Communication in Power Complex Electromagnetic Environment”(No. SGRIXTKJ[2015]796)

然而,由于无线信道的开放性,无线网络面临着诸多威胁,譬如针对无线接口和网络接口的攻击,针对终端和用户识别模块的攻击等,攻击者利用协议缺陷和系统漏洞对网络进行窃听和非法访问,使通信数据泄露、网络服务中断,给通信各方造成各种各样的损失^[2]。与此同时,电网信息涉及电力安全、用户隐私,如果泄露,会造成巨大影响。鉴于此,必须首先研究电力 4G 无线网络的安全防护技术,解决通信、信息安全问题,进而推动电力 4G 网络的大规模推广应用。

2 电力无线网络应用模式

无线技术在电力系统中有两种应用模式:电力无线专网应用模式和电力无线公网应用模式。电力无线公网应用模式是指电力公司租用电信运营商的无线终端及通信信道进行电力数据传输;电力无线专网是指电力公司利用 230 MHz、1.8 GHz 等可用于电力行业的无线频段建设电力无线专网。

2.1 电力无线公网应用模式

利用无线公网承载电力业务具有前期投资少、快速部署、灵活的优势,是公司配电自动化业务的重要通信方式之一。目前,各地电力公司累计租赁了大量公网系统的通信终端及通信信道资源。目前,电力公司租用电信运营商的公网资源主要是 GPRS 网络。

无线公网在电力系统中的应用如图 1 所示^[3],采用无

线公网方式接入信息内网的各类现场终端设备,通过配置运营商的无线公网 APN(access point name,接入点名称)业务,经由无线基站接入公网核心网,再经过核心网网关以公网/专网方式接入系统主站。其中,公网方式是经由互联网连接系统主站;专网方式是通过建立的企业专线经由 APN 接入路由器接入系统主站。

APN 是由电信运营商分配给互联网服务提供商或其他企事业单位的、与其固定 Internet 域名一样的标识,它兼顾了公网的便捷和专网的安全,是一种介于公网与专网之间的虚拟专网(VPN)的业务。面向企业用户,APN 业务就是采用 IPSec VPN 技术,通过 Internet 或建立的 GRE(generic route encapsulation,通用路由封装)专线,为企业、特定行业提供高效的远程互联业务。

APN 业务提供的安全保障措施包括以下 3 点:运营商侧对卡是否合法进行判定;运营商侧对于卡使用的 APN 是否合法进行判定;支持在终端至企业内网侧间叠加加密算法。

2.2 电力无线专网应用模式

由于公网租赁费用高、网络维护缺少主动权等原因,国家电网公司及南方电网公司均开展了电力无线专网技术研究,并建立了试点应用^[4,5]。电力无线专网采用的体制主要包含 MicWILL 技术、TD-LTE 技术等。目前,我国主要推进 LTE 电力专网的建设。

电力 LTE 专网包括 TD-LTE 230 MHz 专网和 TD-LTE

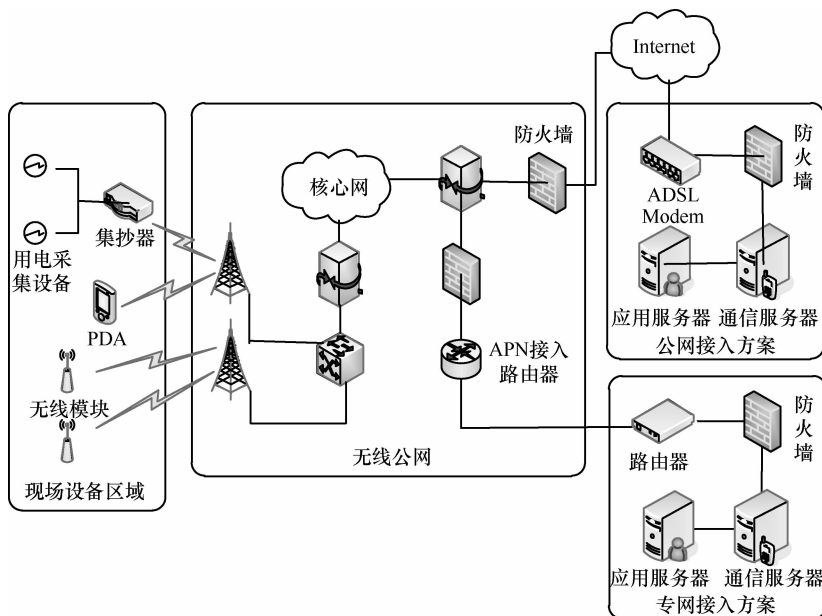


图 1 无线公网在电力系统中的应用

1.8 GHz 专网,它们分别是在 230 MHz、1.8 GHz 频段上组建的 TD-LTE 专网。目前,南方电网公司已在珠海建立了 TD-LTE 1.8 GHz 电力无线宽带专网,国家电网公司在河北开展了 LTE 230 MHz、TD-LTE 1.8 GHz 试点建设。

3 电力 4G 网络安全风险分析

无线通信网络存在以下安全风险:拒绝服务攻击、中间人攻击、非法接入、重放攻击、数据篡改、伪装、窃听、无线链路干扰、物理攻击、隐私泄露、去同步攻击^[67],具体见表 1。

表 1 移动蜂窝通信网络安全风险

安全风险	描述
拒绝服务攻击	有意地造成服务器/网络不能正常运转,致使其不能向合法用户提供所需服务
中间人攻击	攻击者与终端和基站分别建立独立的联系,并交换其所收到的数据
非法接入	非法用户接入已有网络,享受网络服务或合法用户接入私自安装/攻击者设置的接入点
重放攻击	攻击者不断恶意或欺诈性地重复一个有效的数据传输
数据篡改	攻击者获取发送端发送的数据后进行修改、增加或删除,再发送至接收端
伪装	非法用户伪装成合法用户,获得访问关键数据或更高层访问权限的行为
窃听	攻击者通过对网络中的某些设备(信道或节点)的监听来收集信息
无线链路	攻击者通过被动侦听以获取当前网络节点的通信频段,并有意地进行干扰
物理攻击	通过物理手段(如借助特殊的仪器设备)破坏终端或者基站
隐私	窃取终端的身份、位置、地址等信息
去同步	破坏终端和基站间的同步

和 2G/3G 网络相比,4G 的安全架构从复杂性和安全性上来说都有较大提升:提供了基本的用户认证、密钥生成、算法协商、加密和完整性保护功能,为 LTE 系统提供基本的端到端的安全保护体系;提供切换时的密钥更新、网络域安全保护机制等进一步的安全保护功能,提升了 LTE 系统的安全性;提供网络演进中过渡场景下的安全保护机制,如 MME 与 GPRS 服务支持节点(serving GPRS supporting node,SGSN)合设时的安全解决方案等。但是,4G 通信网络具有一些特定的安全风险^[8],主要包括以下几个方面。

(1) LTE 全 IP 系统架构带来的安全风险

LTE 采用基于 IP 的扁平化网络架构,和 GSM 及

UMTS 网络相比,更容易受到数据注入、修改、窃听、隐私泄露等安全威胁。已有参考文献表明 LTE 更易受到 IP 地址攻击、拒绝服务攻击、病毒、木马、垃圾邮件攻击等^[9]。

(2) 家庭基站带来的安全风险

LTE 网络为异构网络,允许部署低成本的家庭基站。这些家庭基站很容易被攻击者攻破,进而伪装成基站或者用户终端对 LTE 网络进行攻击。此外,这些家庭基站不像传统基站那样采用物理保护方法,更易受到物理攻击^[10]。

(3) 多元化终端带来的安全风险

4G 网络的终端不仅仅局限于手机和数据卡,开始逐步泛化,并向汽车、安防、家居等其他领域渗透。新形态的终端接入网络的安全防护系统还不够完善,给黑客带来了可乘之机。

4 电力 4G 网络安全防护需求及防护措施

4.1 电力 4G 网络安全防护需求

除了需要满足传统无线网络数据的机密性、完整性保护等安全防护需求,应对窃听、伪装、篡改、重放等安全风险之外,电力 4G 网络还需要满足电网业务相关的安全防护需求。

(1) 生产控制大区业务的安全防护要求包括访问控制、安全接入、入侵检测

访问控制指生产控制大区与管理信息大区业务间、控制区业务系统与非控制区业务系统间的隔离,采用公网/专网传输时的公网/专网前置机、边界防护设备的安全隔离、加密、认证功能。安全接入指禁止未授权的节点接入骨干网进行业务系统应用、对业务终端身份进行鉴别和控制、制定用户登录错误锁定及会话超时断开等安全策略。入侵检测指监测入侵行为、防止使用常用端口传输恶意信息,防止对服务器发动应用层攻击,在入侵发生时记录入侵的源 IP 地址、攻击类型、攻击目的、攻击时间,并在发生严重入侵事件时提供告警。

(2) 管理信息大区业务的安全防护要求包括访问控制、安全接入、入侵检测

访问控制指内网主站业务系统与外网相关业务系统间的隔离、终端的认证和加密、网络与应用层面的访问控制、边界网络访问控制等。安全接入指仅允许通过认证的终端访问应用系统,实现终端身份认证、安全准入和数据安全交换。入侵检测指对于流经边界的信息流进行入侵检测,在入侵发生时记录入侵的源 IP 地址、攻击

类型、攻击目的、攻击时间,并在发生严重入侵事件时提供告警。

(3)终端设备应配置终端安全模块

对重要终端配置具有双向认证加密能力的终端安全模块,具备对来源于主站系统的控制命令和参数设置指令进行安全鉴别和数据完整性验证的功能;终端上行数据应通过终端安全模块生成摘要,使用对称算法计算相关校验值,供主站识别数据传输的完整性。终端与主站之间应用层通信应具备身份认证、抗重放、数据加密、数据完整性验证等安全功能,有效抵抗网络信息窃听、网络数据篡改、网络重放攻击等威胁,确保数据的传输安全。

4.2 电力 4G 网络安全防护措施

根据电网不同安全分区特点,电力 4G 网络需要对生产控制大区和管理信息大区分别设计,重点在主站侧、终端侧和边界处进行防护。对于所承载的业务及新增业务系统,根据其所属安全分区,参照安全接入方案,采取与安全分区相对应的防护措施进行防护。安全接入方案为主站和终端之间的数据交互提供端对端的安全防护,通过在主站和终端之间进行身份认证、数据加密、数据解密、数据签名等安全防护机制,确保主站和终端之间数据的保密性、完整性和可用性,从而实现信息的防泄露、防篡改,杜绝终端的重放、接管等恶意攻击。

图 2 给出了电力 4G 网络的安全部署,可以看出,无论使用电力专网或者电力公网,均应通过安全接入网关和电

力业务网相连。安全接入网关可实现对电力应用系透明的安全保护,它通过安全通道获取电力应用终端网络数据分组,通过分析网络数据分组进行权限裁决、记录审计日志等,并根据终端权限将网络数据分组转发到电力应用服务器;同时通过网络层获取电力应用服务器网络数据分组,并将网络数据分组通过安全通道转发到终端安全模块。此外,电力 4G 终端均需配置安全模块,具备密码运算服务及安全协议处理功能。可以处理与安全接入网关间的安全协议,包括密钥协商、隧道建立、更新等功能。

此外,电力 4G 网络应采取以下安全防护措施。

(1)防护物理硬件

提升集成度,减少可被攻击的物理接口;增加电流、电压检测电路,防止物理攻击手段;增加完整性检验、可信启动和存储保护等措施^[1]。

(2)实现双向认证

不仅基站可以完成对终端的认证,终端也可以完成对基站的身份认证,对抗伪装、非授权接入等安全风险。

(3)低开销加密

加密是保障数据完整性、机密性的一项重要手段,电力 4G 网络对控制信令和数据信息均进行加密。由于电力存在较多的短数据信息,研发低开销的加密算法十分重要^[8]。

5 结束语

本文针对 4G 技术应用于电力通信网络时存在的各种

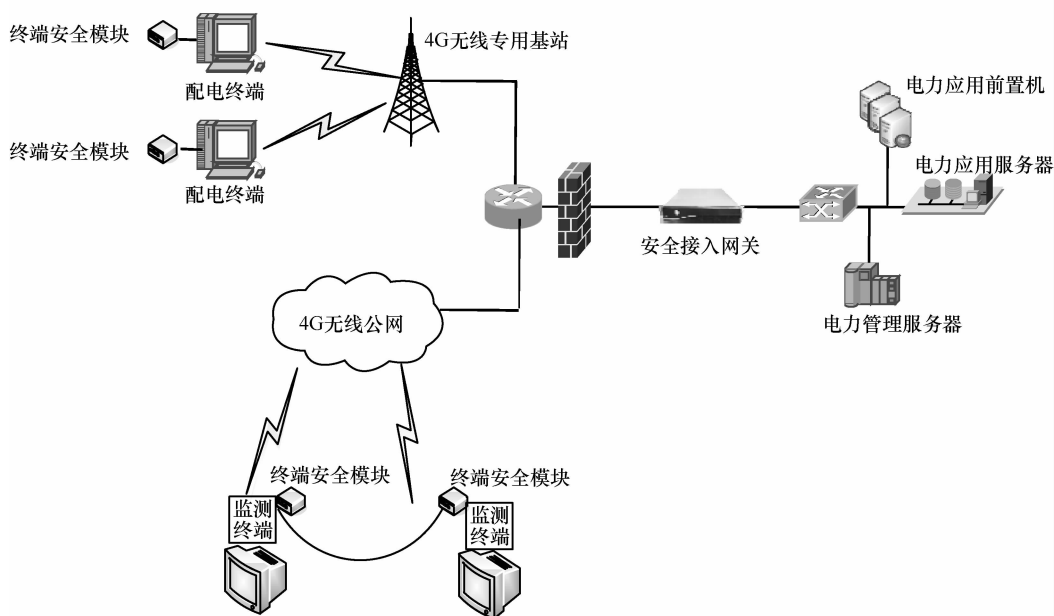


图 2 电力 4G 网络安全部署示意

安全风险问题,提出了配置安全接入网关以及为终端配置安全模块,实现了物理防护、双向认证和数据加密,提高了电力 4G 网络的安全性。

参考文献:

- [1] ASTELY D, DAHLMAN E, FURUSKAR A, et al. LTE: the evolution of mobile broadband [J]. IEEE Communications Magazine, 2009, 47(4): 44-51.
- [2] 黄秀丽, 张涛, 王玉斐, 等. 电力系统通信中 WWAN 安全研究[J]. 计算机技术与发展, 2012, 22(5): 245-249.
HUANG X L, ZHANG T, WANG Y F, et al. Research of WWAN security in communication of power system [J]. Computer Technology and Development, 2012, 22(5): 245-249.
- [3] 国家电网公司. 无线公网安全防护技术研究报告[R/OL]. [2015-10-10]. <http://www.doc88.com/p-6641237805434.html>.
State Grid. Research report on security protection for wireless public network application [R/OL]. [2015-10-10]. <http://www.doc88.com/p-6641237805434.html>.
- [4] 李金友, 闫磊, 齐欢, 等. 基于 LTE230 系统的电力无线通信专网研究与实践[J]. 电气技术, 2014(1): 132-134.
LI J Y, YAN L, QI H, et al. Research and application on the power wireless communication network based on LTE 230[J]. Electrical Engineering, 2014(1): 132-134.
- [5] 曹津平, 刘建明, 李祥珍. 面向智能配用电网络的电力无线专网技术方案[J]. 电力系统自动化, 2013, 37(11): 76-80.
CAO J P, LIU J M, LI X Z. Wireless communication network for intelligent power distribution and utilization system [J]. Automation of Electric Power Systems, 2013, 37(11): 76-80.
- [6] SEDDIGH N, NANDY B, MAKKAR R, et al. Security advances and challenges in 4G wireless networks [C]//The 8th Annual International Conference on Privacy, Security and Trust, August 17-19, 2010, Ottawa, ON, Italy. New Jersey: IEEE Press, 2010: 62-71.
- [7] YANG M H. Security analysis of application layer protocols on wireless local area networks [J]. Journal of Shanghai Jiaotong University, 2011, 16(5): 586-592.
- [8] CAO J, MA M, LI H, et al. A survey on security aspects for LTE and LTE-A networks [J]. IEEE Communication Surveys & Tutorials, 2014, 16(1): 283-302.
- [9] PARK Y, PARK T. A survey of security threats on 4G networks [C]//IEEE Globecom Workshops, November 26-30, 2007, Washington, DC, USA. New Jersey: IEEE Press, 2007: 1-6.
- [10] Rationale and track of security decisions in long term evolved (LTE) RAN/3GPP system architecture evolution (SAE): 3GPP TR 33.821 V9.0.0: 2009[S/OL]. [2015-10-20]. <http://www.qtc.jp/3GPP/Specs/33821-900.pdf>.
- [11] 苗健. 基于 4G 通信技术的无线网络安全通信分析 [J]. 电子技术与软件工程, 2015(1): 43-44.
MIAO J. Analysis on the wireless communication network security based on 4G technology [J]. Electronic Technology & Software Engineering, 2015(1): 43-44.

[作者简介]



李坚(1987-),男,国网冀北电力有限公司工程师,主要从事电力信息安全研究与管理工作。



刘昀(1980-),女,博士,国网冀北电力有限公司信息通信分公司高级工程师,主要从事电力市场、信息通信安全等工作。



安春燕(1987-),女,博士,全球能源互联网研究院工程师,主要从事无线通信、电力线载波通信、通信安全技术研究工作。



任建伟(1980-),男,国网冀北电力有限公司信息通信分公司高级工程师,主要从事电力通信安全研究与运维工作。