 DOI: https://doi.org/10.12345/gcjsygl.v9i18.32647

Research on security protection technology of power communication network

Sixue Zhan

State Grid Hulunbeir Power Supply Company, Hulunbuir, Inner Mongolia, 021000, China

Abstract

As the critical infrastructure ensuring the secure and stable operation of power grids, the protection system of power communication networks plays a vital role. This paper focuses on constructing a security protection technology framework and exploring key technologies for these networks. First, it analyzes the composition, characteristics, and diverse security threats faced by power communication networks, subsequently designing a layered defense architecture. Second, it examines network optimization techniques including structural improvements, boundary isolation, and intrusion detection, along with core data security measures such as encryption and access control. Third, it explores proactive security management and early warning mechanisms that integrate situational awareness, security auditing, and emergency response. Finally, it addresses challenges and future trends in adopting new technologies, aiming to provide theoretical support for building a resilient and reliable cybersecurity defense system for power communication networks.

Keywords

power communication network; security protection; defense in depth; data encryption; situation awareness

电力通信网的安全防护技术研究

展思雪

国网呼伦贝尔供电公司，中国·内蒙古 呼伦贝尔 021000

摘　要

电力通信网是保障电网安全稳定运行的神经中枢，其防护体系至关重要。本文聚焦于电力通信网安全防护技术体系的构建与关键技术研究。首先，文章剖析了电力通信网的组成、特性及其面临的多元安全威胁，并据此设计了纵深防护体系框架。其次，重点研究了网络结构优化、边界隔离、入侵检测等网络安全技术，以及数据传输加密、访问控制等数据安全核心手段。进而，探讨了融合态势感知、安全审计与应急响应的主动式安全管理与预警机制。最后，对新技术引入带来的挑战与未来发展趋势进行了展望，以期为构建韧性可靠的电力通信网络安全防御体系提供理论支撑。

关键词

电力通信网；安全防护；纵深防御；数据加密；态势感知

1 引言

电力通信网是支撑智能电网稳定运行的专有网络，担负继电保护、安全自动控制、调度指挥等重要业务，它的安全性直接影响到国家电力设施的安全性以及国民经济能否顺利进行。伴随着电网智能化、网络化的逐步发展，电力通信网虽然提高了效率以及灵活性，但是它也面临着愈加严重的安全问题。传统的边界防护模式不能应对高级持续性威胁以及内部风险，打造一个多层次的，积极的综合安全防护系统已经成为行业的一种共同认识和迫切的需求。本文主要是对电力通信网络安全风险进行系统的分析，并在网络安全、数据安全、安全管理等方面探究先进的安全防护技术和办法来提高网络的安全保护能力，保证电力系统的稳定运行。

【作者简介】展思雪（1993–），回族，女，中国山东人，本科，工程师，从事电力通信研究。

2 电力通信网概述

2.1 电力通信网的构成与特性

电力通信网主要分为三大部分，传输网、业务网和支撑网。传输网是最基本的部分，它用光缆、微波、电力线载波等多种传输手段组成一个范围很广的实体网络。业务网具体执行电力应用，比如调度电话网，数据通信网等，直接面向生产控制，支撑网涵盖时钟同步网以及网管网，给整个通信网络稳定运行给予保证。

这个网络有着自己的特点，一是可靠性要求非常高，要是出现中断就会直接影响电力的生产和控制工作。二是技术体制多样化，网络中同时存在 TDM、IP 等多种技术制式，复杂性增大。业务隔离性，依照安全分区原则，不同的安全等级的业务要在逻辑上或者物理上严格地隔离开来。业务隔

离性既是安全的要求也是它独有的网络结构形式。

2.2 电力通信网安全风险评估

电力通信网存在的安全威胁来源多样、种类繁多。从物理层面上看，自然灾害或者人为因素会引发电力通信网络线路故障、设备损坏等现象，从而造成基础联通的破坏。从网络的角度来看，拒绝服务攻击、非法接入、网络嗅探会使得带宽用完、非授权的访问或者机密数据外泄。数据和业务层面的风险也更加严峻，攻击者可以伪装成合法的节点注入假的控制命令来误导调度决策，造成一系列连锁故障。病毒、恶意软件会传播到网络里，破坏主机和网络设备正常工作。内部人员误操作或者故意为之也会造成很大危害，能够 bypass 外部非常严密的防护。

3 网络安全防护技术

3.1 网络结构安全

网络安全结构的安全性为整体安全打下基础，它所追求的就是能够实现网络拓扑既稳固又便于维护的目的。第一要事便是实施科学的逻辑分域，在各个安全区之间配置必需的隔断设备来保证各区域严格地按照“安全分区”的规范执行下去。核心层、汇聚层和接入层之间应该有清晰的分层关系，防止出现复杂的网状连接情况，降低故障排查及安全管控难度。第二在网规网设的时候就要考虑冗余性与可靠性。用环形、双路接入等方式形成拓扑，使得出现单点故障不会造成大面积的业务瘫痪。同时，对网络设备自身进行安全配置的加固，关闭不必要的服务端口、使用强密码策略、限制管理权限等，从源头上缩小攻击面，提升网络自身的抗攻击能力。

3.2 边界安全防护

边界安全防护属于抵御外部威胁的第一道防线，它的关键之处在于准确掌控各个信任区域之间流动的数据。横向隔离属于电力通信网最具特色的一种边界防护手段，一般会经由部署正反向隔离装置的方式来达成，在其中运用协议剥离以及内容重组的技术手段，从而完全切断穿透性的 TCP 连接情况出现的可能性，以此保障生产控制大区同管理信息大区之间可以安全地交换数据。纵向边界的防护重点放在上下级调度中心之间通道的安全上，在这里要部署加密认证网关来对所有的远程通信数据做强制性的加密和身份认证工作，从而防止数据的窃听或者篡改，保证接入点是可信的。防火墙是一种普遍适用的边界控制装置，要依照“最小权限”来制定严格的访问控制策略，并对穿过边界的每一份信息进行过滤。

4 数据安全防护技术

4.1 数据传输加密

数据在传输过程中会受到监听、篡改、重播等多种攻击威胁，而保证其机密性与完整性的关键技术就是加密技术。对于调度数据网这样的关键业务，要采用国密算法这类强加密算法，对传输通道实施全程加密，保证数据从起点到终点的整段旅程都是密文状态，即便被截获也无法破译。加密的方式有好几种，IPSecVPN、SSLVPN 属于比较典型的网络层和传输层的加密方法，在 TCP/IP 通信中提供透明的安全防护。对于一些具体的业务应用，在应用层可以集成加密模块，从而实现端到端的安全保障。密钥管理是加密系统安全的基础，要建立完善的密钥生成、分发、更新和销毁机制，防止密钥泄漏。

4.2 安全认证与访问控制

保证操作人员以及访问设备的身份真实可靠是阻止未授权接触的先决条件，诸如数字凭证，动态口令，生物辨认之类的安全识别技术给予了使用者和装置强有力的身分证明办法。电力通信网里，特别要达成数字证书双向认证，也就是服务器既验证客户端的身份，又让客户端验证服务器的身份，以此抵挡钓鱼和伪冒攻击。而访问控制则是建立在认证的基础上，遵循着“最小权限”的原则给用户和程序赋予合适的访问权限。采用基于角色的访问控制模型是最广泛的一种有效的方式，它将权限与角色绑定起来，通过给用户分配角色从而获得相应的权限，极大简化了权限管理。运维操作应该采用权限分离、操作审计的方式，并保证所有的重要的操作都可以被追踪到，以此达到对抗内鬼的目的。

5 安全管理与预警

5.1 安全态势感知

安全态势感知是达成主动防御的关键支撑，它借助对网络里安装的各种安全设备，系统日志，流量数据以及外界的威胁情报展开大量搜集并融合分析，从整体角度即时评判出网络的安全状况和潜藏风险。它能找出那些看上去彼此毫不相干的安全事件背后存在的联系，揭露复杂的攻击链条。一个有效的态势感知平台不仅能做可视化显示，给人们展现全局安全威胁概貌，而且还能依靠大数据分析和机器学习算法对海量数据实施深入挖掘，从而做到针对未知威胁的预先猜测和对异常行为的提前警报。这样就可以让安全管理人员由被通知有告警而变为能够主动去研判风险，从而能够在风险发生之前就先做出防御性的工作，在一定程度上提升了安全运营的效率及前瞻性。

5.2 安全审计与评估

持续的安全审计与评估是验证防护措施是否有效的关键步骤，也是发现系统脆弱性的必要环节，安全审计通过对用户、设备以及应用程序活动日志进行记录并加以分析，来审查安全策略的符合性情况，并找出其中存在违规操作或者异常行为。日志应该集中存放，关联分析以发现潜在的攻击痕迹。而定期开展安全风险评估则是更全面和系统的。它利用漏洞扫描、渗透测试以及基线检测等技术手段，可以主动地去发现网络、系统以及应用当中存在的一些安全隐患问题和配置上的缺陷情况。评估结果要成文报告，明示出风险级

别并给出改进意见。经由定期检查和评价以后，可以不断改善安全制度，促使安全管理程序得到改进，达到动态、不断的循环改善状态。

5.3 应急响应与恢复

再严密的防护也存在发生安全事件的可能性，所以构建起高效的、有条不紊的应急响应及恢复机制十分关键。应急响应就是建立一个事先设定好的组织架构和处理流程，包含事件监测发现、分析研判、遏制消除、恢复重建以及总结改进等一连串步骤。预案是响应的指南，不同的场景需要详细的应急预案，并定期组织演练，让相关人员熟悉流程。事件发生之后应该马上隔离受波及的系统，避免影响进一步扩散，紧接着需要迅速把主要业务恢复正常运转。此后应当全面探究事故的原因，并对以往的经验加以总结以改善防护体系以及应对计划，以此来提高危机处理能力，加强网络安全性。

6 新技术与展望

6.1 新技术应用挑战

云计算、大数据、物联网以及人工智能这些新科技在电力通信网络上使用了之后，带来能力的提高的同时也产生了新的安全问题。云平台的虚拟化、多租户特性新增加了攻击面，数据的所有权和管理责任边界变得不清楚。物联网终端众多且分散，部署环境复杂，在此情况下自身的脆弱性以及被控制之后形成僵尸网络的风险大幅增加。大数据平台汇集大量敏感数据，成为极有吸引力的攻击对象。人工智能可以赋能安全防护，但其模型也存在遭受数据投毒、对抗性攻击等风险。新的技术打破原有的安全边界的限制，因此需要对现有的安全策略以及管理方法做出彻底的调整，并且要能够及时发现和控制由此产生的新风险。

6.2 安全防护发展趋势

未来的电力通信网安全防护将会向着智能化、集成化以及服务化的方向发展，其中智能化就是说安全系统会大量使用人工智能和机器学习算法来自动完成威胁的检测、回应和预判，并且减少对于人工分析的依靠程度。集成化，就是破除安全孤岛，把分散的安全能力统一到一个管理平台上，形成合力。安全即服务的模式将会普及，企业可以像使用云服务一样去订阅自己需要的安全能力，减少企业的部署和维护的成本。零信任架构理念会被更加彻底地付诸实行，“从不信任，一直验证”的核心观念会改变访问控制的方式。另外像隐私计算、区块链之类的，也可能在身份管理、数据追查这些方面起到很重要的作用，促使安全防护朝着更深一步的方向发展。

6.3 未来研究方向

面向未来电力通信网安全防护研究方面有几个重点方向，一是针对新型网络架构的新型网络安全问题的研究，比如在电力中应用的新架构有软件定义网络以及 5G 切片网络等，在这些新型网络架构下的安全性如何实现，其控制器是否安全、切片能否做到隔离性。智能安全运维研究是运用人工智能来实现精准异常检测、自动化的渗透测试和智能化攻防演习。二是内生安全技术研究，探索把安全能力融入到电网业务系统及通信协议之中的新途径，做到安全与业务的深度融合。最后就是安全威胁情报的共享和利用机制研究，怎么做到既能不泄露自己敏感的信息，又能跟大家高效、可信地共享情报，从而共同提高整个行业的防御水平。

7 结语

电力通信网安全防护属于技术，管理以及策略的综合系统工程，面对愈发繁杂的网络威胁及新技术融合所引发的难题，创建纵深化且智能化的主动防御体系成为主要目标。本研究从网络、从数据、管理及未来趋势等多角度出发去研究关键防护技术，其目的是为建立韧性可靠的防御系统提供一定的参考思路。未来应该要不断推进技术革新，加强安全管理的闭环与协同工作，让静态边界的防御模式向动态的零信任架构转变，在此过程中为智能化电网平稳运行奠定稳固的基础。

参考文献

[1] 赵东升,赵旭升,彭玉清.现代电力通信网的安全防护措施研究[J].中国新通信,2025,27(03):4-6+41.

[2] 赵凝.电力系统信息通信网络的安全防护策略探讨[J].电子元器件与信息技术,2022,6(01):255-256.

[3] 姜俐化,夏元斗,戚欣革.电力无线通信网安全防护研究[J].东北电力技术,2020,41(11):23-25.

[4] 甄创和.电力通信网数据安全防护方案分析研究[J].通信电源技术,2020,37(09):203-205.

[5] 黄毅.电力信息通信网安全防护技术措施初探[J].中国新通信,2020,22(02):36.