电力信息网络安全防护技术与防攻击机制研究

刘 妍 孟艳群 冯妍妍 陈若男
国网河南省电力公司郑州供电公司，河南 郑州 450000

[摘要]随着电力系统的智能化和信息化发展，电力信息网络面临着越来越复杂的安全威胁。文章研究了电力信息网络的安全防护技术与防攻击机制，分析了电力信息网络常见的安全威胁与攻击方式，探讨了防护技术的理论基础与实施方法。通过对现有安全防护措施的评估，提出了针对电力信息网络特性的新型防攻击策略，旨在提升电力信息网络的安全性与稳定性。本研究为电力信息网络安全防护技术的研究与实践提供了有益的理论支持和技术指导。

[关键词]电力信息网络；网络安全；防护技术；攻击机制；智能电网
DOI：10.33142/sca.v8i5.16444 中图分类号：TP393.18 文献标识码：A

Research on Security Protection Technology and Attack Prevention Mechanism of Electric Power Information Network

LIU Yan, MENG Yanqun, FENG Yanyan, CHEN Ruonan
Zhengzhou Power Supply Company of State Grid He'nan Electric Power Company, Zhengzhou, He'nan, 450000, China

Abstract: With the development of intelligence and informatization in the power system, the power information network is facing increasingly complex security threats. The article studies the security protection technology and attack prevention mechanism of power information network, analyzes the common security threats and attack methods of power information network, and explores the theoretical basis and implementation methods of protection technology. By evaluating existing security measures, a new anti attack strategy targeting the characteristics of the power information network has been proposed, aiming to enhance the security and stability of the power information network. This study provides useful theoretical support and technical guidance for the research and practice of power information network security protection technology.

Keywords: electric power information network; network security; protective technology; attack mechanism; smart grid

引言

随着智能电网的建设与电力信息化的推进，电力系统的运行与管理日益依赖信息网络。然而，信息网络的开放性和复杂性使得电力信息系统面临着来自外部和内部的各种安全威胁，尤其是网络攻击和数据泄露问题。电力信息网络一旦遭到攻击，不仅会导致经济损失，还可能对电力供应的可靠性和安全性产生严重影响。为了保障电力系统的正常运行，研究电力信息网络的安全防护技术和防攻击机制显得尤为重要。本文旨在探讨电力信息网络的安全防护技术与防攻击机制，以应对日益严峻的网络安全挑战。

1 电力信息网络的安全威胁与攻击机制

1.1 电力信息网络的构成与功能

电力信息网络是支撑现代电力系统运行的关键基础设施，主要由电力设备监控、控制系统、通信网络、数据存储与处理系统组成。它通过智能传感器、自动化控制设备以及信息通信技术（ICT）实现对电力设备和系统的实时监控与管理。电力信息网络通常涉及大规模的区域性与全球性的网络架构，包括变电站自动化系统、智能电表、负荷调度管理系统等，确保电力生产、输配和消费的高效、可靠和安全运行。随着智能电网的逐步部署，电力信息网络在提高电力系统灵活性与可持续性方面发挥着重要作用。然而，随之而来的信息安全问题也日益凸显[1]。

1.2 常见的网络安全威胁与攻击方式

电力信息网络面临多种类型的网络安全威胁与攻击方式，主要包括：

网络病毒与恶意软件：网络病毒与恶意软件是电力信息网络最常见的威胁之一。恶意软件能够通过网络传播并入侵电力系统的各个环节，导致系统瘫痪、数据丢失或设备故障。例如，病毒可以破坏电力调度系统的稳定性，影响设备运行和负荷管理，从而引发电力供应中断等问题。拒绝服务攻击（DDoS）： 拒绝服务攻击（DDoS）是通过大量恶意流量涌向目标电力信息网络设备，使其无法正常提供服务。DDoS 攻击通常针对网络入口点或通信设施，通过大量的虚假请求消耗网络带宽、计算资源或其他系统资源，使得电力信息网络的正常通信中断，影响电力数据的及时传输与系统响应，甚至造成电力生产与配电的停滞。

数据泄露与篡改：电力信息网络中包含大量的敏感数据，包括用电量数据、设备运行信息、调度数据等。数据泄露或篡改不仅威胁到用户隐私和企业机密信息，还可能导致电力调度错误或设备故障。

1.3 电力信息网络攻击的潜在风险与危害

电力信息网络受到攻击所带来的潜在风险与危害极为严重。首先，供应中断是最直接的后果。通过攻击电力信息网络，攻击者可以使电力调度系统瘫痪，从而造成大范围的停电事故，严重影响社会和经济的正常运作。其次，设备损坏与数据丢失也是电力信息网络遭受攻击时可能发生的后果。例如，恶意软件可以破坏电力设备的控制系统，导致电力设备损坏或误操作，增加维护成本并缩短设备寿命。再者，安全隐患加剧，电力系统的安全性一旦被破坏，可能为进一步的攻击和恶意行为提供机会，产生连锁反应，影响到多个电力系统的稳定性。最后，社会信任与法律风险也会加剧。电力信息网络遭到攻击后，用户的隐私数据可能被泄露，损害用户信任；同时，电力企业可能面临法律诉讼与赔偿风险，损害企业声誉，甚至影响国家能源安全。

2 电力信息网络的安全防护技术

2.1 防火墙与入侵检测系统

防火墙和入侵检测系统（IDS）是保护电力信息网络免受未经授权访问与攻击的关键技术。防火墙通过监控并控制进出电力网络的数据流量，阻止恶意访问与不安全的流量，确保只有合法的通信能够进入或离开电力信息系统。防火墙通常配置在电力网络的边界，用于过滤不符合安全策略的网络请求。入侵检测系统（IDS）则负责实时监控网络流量与系统日志，识别并响应潜在的恶意活动，如异常流量、非法入侵或恶意软件的传播。IDS 可以通过特征匹配或异常行为分析的方式检测攻击，并发出警报，为安全人员提供及时的响应机会[2]。

2.2 加密技术与身份认证机制

加密技术和身份认证机制是保障电力信息网络数据传输与访问安全的重要手段。加密技术通过对敏感数据进行加密处理，即使数据在传输过程中被截获，攻击者也无法读取其内容。在电力信息网络中，常用的加密算法有对称加密（如 AES）和非对称加密（如 RSA）。这些加密技术确保了电力网络中的控制命令、监控数据等信息的机密性与完整性。身份认证机制则通过确认访问者身份，防止未授权用户对系统的访问。

2.3 网络访问控制与权限管理

网络访问控制与权限管理是确保电力信息网络内部资源仅对授权用户开放的关键技术。访问控制通过设定严格的权限管理策略，确保不同角色和用户只能访问与其职责相关的系统和数据。例如，利用基于角色的访问控制（RBAC）策略，将用户分配到不同的角色，每个角色拥有特定的访问权限，从而实现细粒度的资源访问控制。同时，权限管理可以通过定期审计用户访问记录、及时撤销离职人员的权限、并控制数据访问的最小权限原则来减少潜在的内部威胁。

2.4 数据备份与恢复技术

数据备份与恢复技术是电力信息网络防范数据丢失与系统崩溃的重要手段。定期备份是保障电力信息网络数据安全的基本要求，尤其是对电力调度数据、设备运行数据等重要信息进行高频次的备份。备份数据可以存储在本地、远程服务器或云平台上，并应采取加密保护措施，防止数据在备份过程中被篡改或泄露。恢复技术则包括在数据丢失、系统遭遇攻击或发生故障时，通过备份数据快速恢复系统运行。电力信息网络中的灾难恢复计划（DRP）需要做到实时监控和定期测试，以确保在任何突发事件发生时，能够迅速恢复系统，保证电力供应的稳定性与连续性。

2.5 安全漏洞扫描与补丁管理

安全漏洞扫描与补丁管理是防止电力信息网络中的安全漏洞被攻击者利用的重要技术手段。通过定期进行安全漏洞扫描，可以及时发现电力信息系统中存在的漏洞，评估漏洞的风险，并采取相应的修复措施。漏洞扫描工具能够扫描操作系统、应用程序、网络设备等各类系统，识别潜在的安全隐患。补丁管理则是指对已知漏洞进行修补的过程，包括及时安装厂商发布的安全补丁，关闭不必要的端口和服务，确保电力信息网络中的所有设备和软件保持最新的安全版本。结合漏洞扫描与补丁管理，能够有效提升电力信息网络的整体安全防护水平，避免攻击者通过已知漏洞发起攻击。

3 电力信息网络防攻击机制的实施与优化

3.1 防御机制的设计原则与框架

电力信息网络的防御机制设计必须遵循一定的原则，以确保系统能够有效抵御各类网络攻击并维持正常运行。首先，防御深度原则要求在电力信息网络的各个层级部署多层次的防御措施，如物理安全、网络安全、应用安全等。每一层防御措施互相配合，共同降低安全漏洞的风险。最小权限原则强调限制用户和应用的权限，只允许它们访问必要的资源，减少内部威胁和滥用风险。此外，灵活性与可扩展性原则要求防御机制能够适应电力信息网络的动态变化，随着网络规模和复杂度的增加，能够快速应对新的威胁与攻击。最后，持续监控与响应原则则强调对网络活动的实时监控，确保能够及时发现异常行为并采取应对措施[3]。

3.2 防攻击策略的技术选型与实现

基于人工智能的威胁检测与响应:随着网络攻击形式日益复杂，传统的安全防护措施已难以应对新型攻击。基于人工智能（AI）的威胁检测技术利用机器学习和深度学习算法，能够实时分析大量网络流量、日志信息及设备行为，从中识别潜在的安全威胁。AI 技术通过不断学习和优化，可以提高对未知攻击的识别率，减少误报和漏报。

基于区块链的电力数据安全:区块链技术的去中心化和不可篡改的特性，使其成为提升电力数据安全的有效工

具。通过将电力信息网络中的关键数据（如电力交易、设备运行数据等）存储在区块链中，能够确保数据在传输、存储过程中的安全性和完整性。区块链的分布式账本使得数据一旦记录后无法被篡改，极大降低了数据泄露和篡改的风险。

3.3 安全防护体系的综合应用

多层次安全防护是构建电力信息网络安全防护体系的核心思想。它通过在不同的网络层级和系统层面部署多种安全技术，如边界防火墙、入侵检测系统、加密传输、访问控制等，形成纵深防御。在网络层面，防火墙和入侵检测系统（IDS）可以监控和拦截外部的恶意访问；在传输层，使用加密技术保护数据传输的机密性和完整性；在应用层，结合访问控制与身份认证确保只有授权用户才能访问敏感数据。威胁情报共享与协同防御是提升电力信息网络防御能力的重要策略。通过与其他电力公司、行业机构以及国家安全部门共享威胁情报，电力信息网络能够及时获取最新的攻击手段、病毒变种和安全漏洞信息。威胁情报共享不仅提升了电力网络对常见攻击的预警能力，还可以增强整体安全防御的协同性。例如，在发生大规模的 DDoS 攻击时，电力公司可以与其他能源企业共享防御策略，共同抵御攻击，减少损失。

4 电力信息网络安全防护技术的挑战与发展趋势

4.1 面临的挑战与困难

安全资源投入与技术发展不平衡

尽管电力信息网络在现代电力系统中扮演着至关重要的角色，但相较于其他关键基础设施，电力信息网络的安全投入和技术发展仍显不足。许多电力企业在安全资源的配置上往往偏向于物理基础设施的建设，而忽视了信息网络的安全防护。在资金、技术和人才投入上的不平衡，使得一些电力企业未能及时跟上快速发展的网络安全技术，导致其防护能力相对较弱。电力信息网络的环境复杂且高度动态，设备种类繁多，连接方式复杂，涵盖了传统电力系统、智能电网、云计算平台等多个层面。这种高度复杂的网络环境使得安全防护变得更加困难。首先，不同设备和系统的安全标准不统一，导致防护策略的执行上存在差异。其次，电力信息网络中的数据流量庞大，攻击者可能通过多种手段进行分布式攻击，造成数据泄露或系统瘫痪[4]。

4.2 未来发展的研究方向

智能化与自动化防护技术：随着网络攻击手段的不断升级，传统的人工防护方式已经难以应对大规模和复杂的攻击行为。未来，智能化与自动化防护技术将成为电力信息网络防护的重要发展方向。基于人工智能（AI）和机器学习的自动化检测与响应系统，可以实时监控并分析大量网络流量，自动识别异常行为并进行快速反应。通过深度学习和自适应技术，智能防护系统能够不断优化防御策略，提前识别潜在的攻击并自动部署防护措施。这种自动化的防护技术将大幅提升电力信息网络的响应速度和防御能力，减少人为干预和误操作的风险。

跨领域协同与安全策略创新：电力信息网络的安全防护不仅仅是一个单一领域的任务，更需要跨领域的协同合作。未来的研究方向将侧重于建立跨行业、跨领域的安全防护体系。例如，电力企业可以与信息通信、金融、政府等领域的机构合作，共享威胁情报与安全防护经验，提升整体防御水平。高度集成与全面防护:电力信息网络的安全防护将朝着高度集成的方向发展，目标是实现全方位、无死角的安全防护。随着技术的不断进步，防护技术不再是孤立的，而是一个高度集成的体系。电力信息网络中的各类安全防护技术（如防火墙、入侵检测、身份认证、加密技术等）将能够协同工作，形成一个统一的安全防护平台，实现对电力系统的全方位监控与防护。

5 结束语

随着电力信息网络的日益发展，安全问题已成为保障电力系统稳定运行的关键。本文通过分析电力信息网络的安全威胁与攻击机制，提出了多种有效的防护技术和防攻击策略。尽管现有的安全防护技术在一定程度上解决了网络攻击问题，但面对日益复杂的网络安全环境，电力信息网络的安全防护仍面临许多挑战。未来，随着技术的不断进步和安全防护机制的不断优化，电力信息网络的安全性将得到更好的保障，为智能电网的稳定运行提供强有力的支持。

这份大纲覆盖了电力信息网络安全防护技术的各个方面，您可以根据这个框架进一步扩展具体内容。如果有更具体的要求或需要修改的部分，随时告诉我！

[参考文献]

[1]黄诗槊.电力系统中计算机网络信息安全的防护研究[J].信息与电脑(理论版),2024,36(17):29-31.
[2]王俊娜,高新平.电力系统计算机网络信息安全防护研究[J].工业控制计算机,2024,37(7):137-138.
[3]谢光南.分析安全隔离技术运用在电力信息网络安全防护中的效果[J].中国新通信,2023,25(1):115-117.
[4]赵宇,金伟.浅谈电力调度数据网网络安全防护技术[J].数字通信世界,2019(6):59.

作者简介：刘妍（1993.3—），女，河南省驻马店市人，汉族，研究生，中级电力工程师，就职于国网郑州供电公司，从事信息系统检修维护工作。