针对电力通信网的信息安全技术研究

张 岩
内蒙古电力（集团）有限公司锡林郭勒供电分公司 内蒙古 锡林浩特 026000

摘 要：随着电力通信网的迅速发展，在信息化建设中，电力通信网已成为智能电网、大数据应用等方面的核心基础设施，对于维护电力行业的稳定运行和安全可靠具有重要意义。然而，由于其特殊性质和特殊需求，电力通信网所面临的威胁与安全问题也日益突出。因此，在电力通信网的信息安全技术研究方面，亟需加强研究，提高信息安全保障能力。

关键词：电力通信网；信息安全技术；研究

引言

电力通信网是电力系统的神经网络，对于电力系统的稳定运行和安全具有至关重要的作用。然而，随着电力通信网的不断发展和完善，它所面临的信息安全威胁也越来越多，其中的黑客攻击、病毒入侵、信息泄露等安全问题，威胁着电力通信网的正常运行和数据的安全[1]。因此，对电力通信网的信息安全技术的研究显得尤为重要。本文将以电力通信网的信息安全技术的研究为主线，介绍了电力通信网的架构、安全威胁、信息安全标准和技术，并介绍了电力通信网信息安全技术的发展趋势。

1 电力通信网的特点

电力通信网是指为电力系统互联的一种通信系统，并且是电力系统中的关键应用。以目前的技术水平来看，电力通信网可以被划分为数字传输系统、保护自动化系统、调度自动化系统和企业办公自动化系统四个方面。数字传输系统是电力通信网的基础，其主要负责电力系统内部各种信号的传输，包括电能计量和监控、保护信号传输和设备的控制信号传输等。保护自动化系统包括数字式保护装置、自动开关和远动设备等，主要负责电力系统的保护和稳定运行。调度自动化系统主要负责电力系统的调度运行和管理。企业办公自动化系统是指企业内部通信和管理信息的系统。电力通信网是指连接电力系统各个部分的网络，包括高压、中压、低压配电、变电站等部分。电力通信网具有以下的特点：1）传输距离较长：电力通信网一般需要将信号传输到较远的地方，这就要求其具备高速率、低误码率等性能。2）网络节点众多：电力通信网涉及众多的网络节点，涵盖了电力系统的各个环节，这就要求它具备高度的兼容性和稳定性。3）应用场景复杂：电力通信网所涉及的应用场景较为复杂，例如智能电网、大数据等领域。这就要求其具备高度的安全性和可靠性。4）信息交换实时性强：电力通信网所涉及的信息交换需要保证实时性和准确性，以便于实现实时监测、控制和调度。

2 电力通信网的信息安全技术的作用

信息安全技术在保障电力通信网的系统安全方面扮演了至关重要的角色。首先，信息安全技术可以有效防止网络安全威胁，如黑客攻击、病毒感染、网络钓鱼等，在形成网络威胁时进行及时拦截和防范；其次，数据安全技术可以对电力通信网中的机密数据和敏感信息进行高强度加密和保护，同时还可以有效防范变速操作和恶意用户的非法访问，保证数据的完整性和机密性；第三，系统安全技术可以对电力系统中的服务器、路由器和全部设备进行持续监测，以及对全部故障进行安全管理，防止系统的意外关闭、虚假输入和恶意攻击等问题；最后，物理安全技术可以加强对设备、服务器、密码品、数据资源和核心部件的校验，以及对灾难和火灾的防范，保证电力通信网的全面安全。

3 电力通信网所面临的威胁

随着电力通信网的发展和普及，它所面临的威胁也不断增加。一些黑客攻击电力通信网，以获取机密信息或者对电力系统进行破坏；一些病毒程序侵入电力通信网，导致电力通信网不稳定，甚至瘫痪。在此基础上，本文重点介绍以下几种电力通信网所面临的威胁：1）黑客攻击：黑客通过攻击电力通信网节点，破坏电力系统的稳定和安全，并利用这种破坏行为来获取非法利益。2）病毒感染：电力通信网受到病毒感染，导致电力通信网不稳定，影响正常监控和保护，对电力系统的稳定和安全构成威胁。3）物理破坏：一些攻击者在电力通信网中的电缆通信线路、信号机箱、互联网关等节点上进行物理破坏，导致通信系统的完整性和安全性遭到破坏。4）信息窃取：电力通信网中包含大量的敏感信息，如电力系统的运行状态信息、设备管理信息和电力运行计划

信息等，这些信息容易被攻击者窃取，造成安全泄漏。

4 电力通信网安全技术

4.1 基于密码学的技术

1）基于密码学的技术在电力通信网络中的应用。电力通信网络中的应用分为两个主要方向：认证和加密。认证是验证通信双方身份的过程，防止骗子伪装成合法用户访问网络。加密则是通过对数据进行加密和解密来保护数据传输的安全性，避免数据泄露。基于密码学的技术能够实现对电力通信网络的数据加密，并能够实现电力通信网络中的数据身份识别。周到的密码保护机制的实现有助于防止数据泄露和别有用心者的非法入侵。2）基于密码学的技术的主要手段。基于密码学的技术的主要手段包括：第一，对称加密。对称加密是指数据发送和接收方共享一个密钥，通过该密钥进行加密和解密，从而保护数据的安全性。第二，非对称加密[2]。非对称加密使用不同的密钥来加密和解密数据，通常被用于数字签名和数字证书。第三，数字签名。数字签名是指对电子文档进行数字签名，使被签署的文档的真实性得到确认并防止伪造。第四，数字证书。数字证书用于验证通信方的身份，它由数字身份证明机构发放，包括证书颁发机构和证书持有人的身份信息。

4.2 防火墙和入侵检测技术

1）防火墙技术。防火墙技术是一种网络安全技术，能够在电力通信网入口和出口处进行协议转换和过滤，阻止未经授权的访问，从而保障电力数据的机密性和完整性。防火墙方式多种多样，最常见的防火墙包括软件防火墙、硬件防火墙及混合防火墙。其中，硬件防火墙是最常用的防火墙之一，主要通过硬件设备进行防护，硬件防火墙具有响应快、拦截能力强和抗攻击能力强等特点。在电力通信网中，防火墙技术不仅能够对风险行为进行检测及防范，还能够实现数据过滤、访问控制和VPN等必要安全功能。因此，防火墙是保障电力通信网信息安全的重要安全手段。通过防火墙的应用，电力通信网中的核心数据得到加密和保护，网站、服务器和电子邮件系统也能够防范黑客、病毒、网络蠕虫等威胁。相对于其他安全技术，防火墙还具备灵活扩展等特点，适用于大多数的电力通信网场景。2）入侵检测技术。入侵检测技术是一种安全监控技术，主要用于实时监控网络中的安全威胁行为，如黑客攻击、恶意软件、网络病毒等。根据入侵检测技术的检测手段，入侵检测技术适合分为基于主机的入侵检测系统和基于网络的入侵检测系统。基于主机的入侵检测系统主要通过计算机系统日志或文件中的信息，并结合预设的规则或特征进行分析、检测和报警；而基于网络的入侵检测系统则主要通过网络流量的检测和分析来进行检测。在电力通信网中，基于网络的入侵检测系统是一种非常重要的安全监控技术，能够扫描网络探测威胁，检测网络攻击，发现网络安全漏洞，并及时向管理员报告安全事件。入侵检测系统应用广泛，可以对于许多电力通信网使用的操作系统（如Windows、Linux、Unix等）、网络协议（如TCP/IP、SMTP、FTP等）和应用程序（如HTTP、IM、邮件等）进行分析。因此，入侵检测技术主要工作是在网络数据上进行处理，通过离线或在线的检测方式，对加密数据、攻击行为等进行有效的监控和检测。

4.3 虚拟专用网络（VPN）技术

虚拟专用网络（VPN）是一种基于公共互联网的专用通信网络，可用于保护数据传输的隐私性和完整性。在电力通信网安全技术中，VPN技术被广泛采用，以保护电力通信网中的敏感数据。VPN技术可以在不安全的公共互联网上建立一个安全的专用通信通道，保证用户数据的安全传输。在电力通信网中，VPN技术将公网上的数据通过加密方式传输，因此，攻击者无法截获数据包，保证了数据的安全性。同时，VPN技术还能够确保数据的完整性、可靠性和机密性，有效预防钓鱼、黑客攻击和非法入侵等安全威胁。在电力通信网的应用中，VPN技术有以下几个特点：1）建立安全通道：VPN技术可以在公网上建立安全通道，通过协议隧道技术来保护数据流，防止黑客入侵和恶意攻击等危险行为。2）安全加密：VPN技术采用高效的加密算法，如AES、DES、3DES等，对传输的数据进行加密，保证数据传输过程中的数据安全性。3）访问控制：VPN技术可以实现针对不同用户进行访问控制策略，控制用户的访问权限，保证数据的机密性。4）弱点覆盖：VPN技术能够覆盖传统的网络短板，实现远程访问，提高网络弱点的安全性。

4.4 网络安全监控技术

网络安全监控技术是电力通信网安全技术的核心技术之一，它可以对电力通信网络进行实时监控和预警，识别并防范各类网络安全风险。网络安全监控技术需要采用一系列技术手段和工具来实现，如应用软件评估、入侵检测、日志监控等，来保障电力通信网络的安全。本文将详细介绍网络安全监控技术在电力通信网中的应用。1）应用软件评估。应用软件评估是指通过网络安全与审计工具从网络主机应用程序的安全角度进行综合评估和分析，以识别主机应用程序存在的安全问题[3]。应用软件评估可以用于确定是否有恶意软件感染、是否存在系统漏洞和是否存在未授权远程访问等风险问题。该项

技术可通过对软件信息的验证、文件完整性检查、源代码扫描、数据包、流量分析、动态调试等技术手段进行分析，从而识别恶意行为并对其进行干预和阻断，保护电力通信网络的安全。2）入侵检测。入侵检测是指在网络主机中的安装安全审计软件，在网络主机上实时分析网络数据以识别异常事件的行为。它利用监控技术对系统的各种行为和数据进行分析，通过安全策略的实现和音频警报的方式进行入侵检测和报警。该技术能够及时发现电力通信网络中非法入侵行为，防范和遏制安全威胁的发生。3）日志监控。日志监控是指通过尽可能地收集和记录不同的系统日志信息，对铁路通信网机房内的操作行为、网络异常事件等进行定期监测和分析，以便于在日后的安全审计中识别网络事件并进行跟踪。日志监控可以有效识别和防范未知的风险和威胁，并及时进行应对和解决。

4.5 安全备份技术

安全备份技术是保障电力通信网数据安全的重要手段之一。电力通信网中的数据是非常重要且具有机密性的，如若数据丢失或损坏，将会给电力通信网带来严重的后果。这时，安全备份技术就可以保证电力通信网的数据得到及时备份，以防数据丢失和毁坏。安全备份技术具有以下几个主要特点：1）实时备份。安全备份技术能够在数据发生变化以及重要数据发生变化时及时地进行备份处理，确保电力数据的安全性和完整性。2）多备份。安全备份技术可以为电力通信网中的重要数据备份多个副本，以应对不同的安全威胁和数据损坏情况，保证数据的安全性。3）灵活性。安全备份技术具有高度的灵活性，可以根据实际需求和条件进行备份处理操作。同时还可以对备份的数据进行分级管理，确保数据安全性的同时，对数据进行科学、合理地规划和管理。

4.6 安全管理技术

安全管理技术是电力通信网及其信息的全面管理，包括信息的access控制、监控、漏洞管理和风险评估等，可通过信息安全管理技术使得电力通信网的信息健康有序地运行，提高电力数据的保密程度，有效地防范电力数据泄露和信息攻击。

5 加强电力通信网信息安全的建议

1）建立健全的安全管理体系。电力企业应该建立一套完整的安全管理体系，包括安全策略、安全流程和安全控制等方面。安全管理体系应该覆盖所有电力通信网相关的工作，包括网络设备的配置、访问控制、日志审计等方面。此外，安全管理体系还需要定期进行风险评估和漏洞扫描，及时发现潜在的安全威胁。2）加强密码学技术的应用。采用加密算法可以对电力通信网中的数据进行加密传输，防止数据被窃取或篡改。同时，使用安全协议如SSL/TLS可以保护通信双方的身份认证和会话完整性。3）优化系统安全配置。针对电力通信网中的不同设备，应该采取相应的安全配置措施。例如，防火墙可以用于过滤恶意流量，VPN可以用于提高通信链路的安全性，入侵检测和防病毒软件可以实时监测和清除系统中的威胁。

结语

总结起来，对于电力通信网的信息安全技术的研究不仅是保障电力系统安全的重要保证，更需要深化技术研究，提高管理水平，并与时俱进地掌握信息安全技术新动向，以应对未来可能出现的新威胁，更好地保障我国电力通信网的安全与稳定。

参考文献

[1]余莉娜,董伟.基于实时检测的电力通信网入侵检测系统研究[J].互联网安全技术,2021,2(1):66-71.

[2]张先平,王超,吕宝林等.基于人工智能的电力通信网安全关键技术研究[J].电力科学与工程,2020,36(6):38-43.

[3]林如璇,罗英华,王子栋等.基于区块链的电力通信网信息安全技术研究[J].安全与通信技术,2019,2(6):59-64.