电力网络安全态势感知与预警系统

王硕暄

（多斯供电公司　内蒙古鄂尔多斯市　017010）

摘要：本文深入研究了电力网络安全态势感知与预警系统，涵盖理论基础、架构设计、关键技术及发展趋势。详细剖析了电力网络安全的重要性、威胁和保障需求，并探讨了态势感知和预警系统原理，以及大数据、人工智能等技术的应用。系统架构部分着重介绍了数据采集、态势分析和预警响应等模块。关键技术研究中，聚焦于数据融合、异常检测、威胁评估和事件关联分析。文末展望了该系统的技术发展动向、政策法规支持及行业应用前景。

关键词：电力网络安全；态势感知；预警系统；大数据；人工智能

引言

随着信息技术进步，电力网络安全的重要性日益凸显，它是保障电力系统稳定运行的关键。面对网络攻击、病毒和数据泄露等威胁，需采取物理、网络、数据和应用等多层面安全措施。态势感知作为预测网络安全变化的重要手段，通过实时监控和分析，助力早期发现威胁。预警系统则是防范安全事件的前沿防线，实时监测并预警，以降低安全风险。技术发展推动大数据、人工智能和机器学习在电力网络安全中的应用，提升了态势感知与预警的效能。本文旨在探讨电力网络安全态势感知与预警系统的理论、架构、关键技术及发展趋势，为电力网络安全提供理论和技术支撑。

一、电力网络安全态势感知与预警系统理论基础

随着计算机、网络和通信技术在智能电网中的广泛应用，现代电力系统已发展成由物理电力系统和监控信息通信系统组成的复杂耦合网络系统[1]。在电力发展过程中，信息网络的安全性至关重要，特别是对于监控信息，而传统电力网络安全的防护技术薄弱，在实际应用中容易产生防护漏洞，导致重要信息泄漏，或者网站信息被篡改等事故的发生[2]。

（一）电力网络安全概述

电力网络安全是保障电力系统稳定运行的关键因素之一。它涉及电力生产、传输、分配和使用的各个环节。电力系统的网络化、智能化程度越高，其面临的网络安全风险也越大。常见的网络安全威胁包括网络攻击、病毒入侵、数据泄露等。为了确保电力系统的安全运行，必须采取有效的安全措施，包括物理安全、网络安全、数据安全和应用安全等多个层面。

（二）态势感知理论

态势感知理论起源于军事领域，旨在通过对环境的持续监控和分析，来预测未来的发展趋势和潜在威胁。在电力网络安全中，态势感知通过对网络流量、系统日志、用户行为等数据的分析，实现对网络状态的实时监控和威胁的早期发现。态势感知通常分为三个层次：感知（收集数据）、理解（分析数据）和预测（预测未来状态）。

（三）预警系统原理

预警系统通过持续监控网络环境，有效识别潜在的安全风险，并迅速发出警报，为实施防御措施争取宝贵时间。在电力网络安全领域，预警系统一般由数据采集、威胁识别、风险评估和报警处理等模块构成，旨在减少安全事件的发生概率及其造成的负面影响。

（四）相关技术概述

大数据技术为电力网络安全提供了海量的数据支持，使得对网络状态的全面分析成为可能。人工智能和机器学习技术则通过算法模型，能够自动识别复杂的攻击模式和异常行为，提高威胁检测的准确性和效率[3]。例如，机器学习算法可以用于训练模型，以识别网络流量中的异常模式，而人工智能可以用于自动化决策和响应过程。这些技术的融合应用，为电力网络安全态势感知与预警系统提供了强大的技术支撑。

二、电力网络安全态势感知与预警系统架构设计

架构设计是电力网络安全态势感知与预警系统的核心，它决定了系统的功能、性能和可靠性。

（一）系统总体架构

系统总体架构采用分层设计，以确保高度的模块化和可扩展性。主要包括以下几个层次：数据采集层、数据预处理层、态势分析层、预警与响应层以及用户界面层。数据采集层负责从电力监控系统、网络设备等源头收集数据；数据预处理层对原始数据进行清洗和格式化；态势分析层利用算法模型分析数据，生成网络安全态势；预警与响应层根据分析结果触发警报并采取相应措施；用户界面层则提供人机交互界面，方便用户监控和管理。

（二）数据采集与预处理模块

数据采集模块负责从多个数据源实时采集网络流量、系统日志、设备状态等信息。预处理模块则对采集到的数据进行去噪、归一化和特征提取[4]，以确保数据的质量和可用性。这一过程是后续分析的基础，对于提高系统整体性能至关重要。

（三）态势分析模块

态势分析模块通过应用机器学习、数据挖掘和统计分析等方法，对网络行为、安全事件和系统漏洞进行深入分析。它能够识别出潜在的威胁模式，评估网络的安全状况，并为预警提供依据。该模块的关键在于构建有效的分析模型和算法，以实现对复杂网络环境的准确理解。

（四）预警与响应模块

预警模块根据态势分析结果，对可能发生的网络安

全事件发出警报。响应模块则根据预警级别和预设的响应策略，自动或手动采取措施，如隔离攻击源、更新防火墙规则、启动应急预案等。这一模块的设计需要考虑实时性和灵活性，以确保在紧急情况下能够迅速有效地应对。

（五）系统集成与测试

系统集成是将各个模块按照设计要求组装成一个完整的系统。这一过程涉及接口匹配、数据流转、功能协调等环节。测试则包括单元测试、集成测试和性能测试等多个阶段，旨在验证系统的功能、性能和安全性是否符合预期。通过严格的测试，可以确保系统在实际运行中的稳定性和可靠性[5]。

三、关键技术研究

在电力网络安全态势感知与预警系统中，关键技术的研究与应用是提升系统效能的核心。

（一）多源数据融合技术

多源数据融合技术通过整合来自不同传感器、网络设备、日志文件等的数据，形成一个统一的、一致的信息视图。这种方法可以消除数据孤岛，提高数据的利用率和分析效率。在电力网络安全中，多源数据融合技术主要包括数据对齐、特征提取、数据融合算法等，它们共同作用，确保了态势感知的全面性和准确性。

（二）异常检测算法

异常检测算法旨在从正常行为中识别出异常模式。在电力网络安全领域，这些算法包括基于统计的方法、基于机器学习的方法和基于深度学习的方法等。例如，孤立森林算法可以快速识别数据集中的异常点，而神经网络则能够学习复杂的非线性关系，用于检测隐蔽的攻击行为。

（三）威胁评估与预警方法

威胁评估是对检测到的安全事件进行严重性评估的过程，它涉及威胁的定性分析和定量计算。预警方法则根据威胁评估的结果，决定何时以及如何发出警报。在电力网络安全中，常用的方法包括基于规则的评估、基于概率的评估和基于风险的评估等。

（四）安全事件关联分析

安全事件关联分析通过分析事件之间的时间序列、因果关系和网络拓扑关系，将看似独立的安全事件联系起来，从而揭示攻击者的整体攻击策略。这种方法在电力网络安全中尤为重要[6]，因为它能够帮助安全团队从大量的安全事件中识别出复杂的攻击模式，如高级持续性威胁（APT）。有效的关联分析不仅提高了威胁检测的准确性，还增强了系统的整体防御能力。

四、电力网络安全态势感知与预警系统发展趋势

随着技术的进步和电力行业的发展，电力网络安全态势感知与预警系统正面临着前所未有的机遇和挑战。

（一）技术发展趋势

随着云计算、物联网、5G 等技术的普及，电力网络安全态势感知与预警系统的发展将呈现出智能化与自动化的趋势，人工智能技术的深入应用将极大提升系统的自动化和智能处理能力。同时，大数据分析技术的成熟将助力态势感知系统获得更精确的决策支持。边缘计算的应用将推动数据处理向数据源靠近，降低延迟，增强系统的实时响应能力。此外，区块链技术的去中心化和不可篡改性特点，预计将提高网络安全事件记录与追踪的可靠性，从而为电力网络安全提供更加坚实的保障。

（二）政策与法规支持

近年来，为了加强网络安全管理，各国政府陆续出台了相关政策法规，包括完善网络安全法律法规体系，为电力网络安全提供法律依据和操作指南。同时，政府通过资金支持、税收优惠等政策扶持措施，激励企业加大网络安全技术的研发与应用力度。此外，还积极推动网络安全标准的制定与实施，以提升系统的互操作性和安全性，从而全面加强网络安全的防护能力。

（三）行业应用前景

随着电力系统复杂性和互联性的不断提升，电力网络安全态势感知与预警系统的应用前景愈发广阔。在智能电网的建设与运营中，该系统将成为确保电网安全稳定运行的核心技术。同时，它将加强对电力监控系统的防护，防止网络攻击引发的服务中断和数据泄露。此外，通过实时监测和预警，系统将显著提升电力企业在应对网络安全事件时的应急响应能力。更进一步，该系统将推动电力行业内外的安全信息共享和协同防御，构建起一个更为广泛和紧密的安全防护网络。

结束语

在信息技术飞速发展的背景下，电力网络安全成为保障国计民生的重要领域。深入研究电力网络安全态势感知与预警系统，不仅确保了电力系统的稳定运行，也为未来网络安全挑战做好了准备。感谢所有研究者的努力，将理论转化为实践。期待更多专家加入，共同推动技术发展。展望未来，我们将持续优化系统，应对网络安全挑战，致力于构建更安全、智能的电力网络安全体系，助力我国电力事业的发展。

参考文献：

[1]张浩,温永亮,孙长春,等.电力监控系统网络安全主动防御研究[J].电气传动自动化,2023,45(04):65-68.

[2]苏生平,刘禹彤.电力监控系统网络安全架构技术研究[J].信息技术,2023,(11):179-183+190.DOI:10.13274/j.cnki.hdzj.2023.11.031.

[3]于斌,刘曦.态势感知系统在电力网络中的应用[J].电子技术与软件工程,2020,(21):221-222.

[4]张佳发,刘家豪,邓远发.入侵攻击下电力信息网络安全态势感知分析[J].电子技术与软件工程,2020,(21):251-252.

[5]谢汉明,米雪峰.电力信息安全技术防护措施探讨[J].电工技术,2020,(17):115-116.DOI:10.19768/j.cnki.dgjs.2020.17.037.

[6]成健,胡力广,詹威鹏,等.电力监控系统网络安全态势感知研究[J].电气应用,2020,39(07):86-89.