基于大数据技术的电力信息系统安全状态监测方法

徐颖 张安吉

（国网武汉供电公司武昌配电运检分公司 湖北武汉 430061；华北电力大学国教院 河北保定 071066）

摘要：随着电力信息系统的日益复杂化和重要性，基于大数据技术的电力信息系统安全状态监测方法的研究显得尤为重要。本文首先阐述基于大数据技术的电力信息系统安全状态监测的重要性，而后分析其基本架构，并详细介绍了基于大数据技术的电力信息系统安全状态监测方法。最后，通过试验与检测验证了该方法的有效性。

关键词：大数据技术；电力信息系统；安全状态监测

引言：在目前的电网建设工作中，现代化已是一个重要方面，尤其是在目前社会对用电需求不断增加的情况下，电力公司的发展需要对大量的数据进行分析；新的机遇与挑战决定着企业未来是否能够持续、持久地发展，而针对这一转变而出现的电力信息系统也在实践中得到了很好的应用，它不仅为各种设备的高科技操作提供了完整的数据基础，而且对降低电网运行的危机具有重要意义。

1 基于大数据技术的电力信息系统安全状态监测重要性

随着我国电力行业的快速发展，电力信息系统的安全问题日益凸显。电力信息系统承载着电力行业的核心业务，涉及国家安全、经济运行和社会稳定等方面。因此，保障电力信息系统安全具有举足轻重的作用。基于大数据技术的电力信息系统安全状态监测在此背景下应运而生，其重要性体现在以下几个方面：（1）增强安全意识：基于大数据技术的电力信息系统安全状态监测有助于提高全社会对电力信息系统安全的认识，从而增强安全意识。通过大数据技术，可以实时监测电力信息系统的安全状态，发现潜在的安全隐患，为防范和应对电力信息系统安全事件提供有力支持[1]。（2）预防安全事件：基于大数据技术的电力信息系统安全状态监测能够实现对电力信息系统安全的全方位、全天候监测，有效预防安全事件的发生。大数据技术可以实时收集和分析电力信息系统中的各种数据，通过对这些数据的挖掘和分析，提前发现安全漏洞和风险，为电力信息系统安全防护提供有力支撑。（3）提高安全防护能力：基于大数据技术的电力信息系统安全状态监测可以提高电力信息系统安全防护的能力。通过大数据技术，可以对电力信息系统进行全面监测，了解系统的实际运行状态，从而有针对性地加强安全防护措施。此外，大数据技术还可以为电力信息系统安全防护提供科学依据，帮助相关部门制定合理的安全策略。

2 基于大数据技术的电力信息系统安全状态监测基本架构

在此基础上，建立了一种基于大数据的电力信息系统安全监控体系结构模型，主要电气设备、变电站总线、网络设备、智能电网等通过对站控系统、调度中心、工作站等设备的运行状况进行实时监控，并将其上载至安全状态监测中心，其结构见图 1。该系统具有对长时间采集的数据进行存储和分析的功能。本项目以电力信息系统安全状态为研究对象，以获取高精度的大数据为研究对象，以模糊聚类为基础，结合博弈理论、增强学习等技术，开展电力信息系统安全状态监控研究，设计原理见图 2。

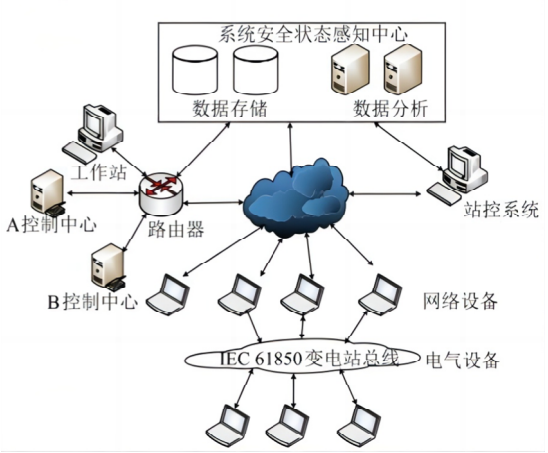

图 1 基于大数据分析的电力信息系统安全状态监测技术架构

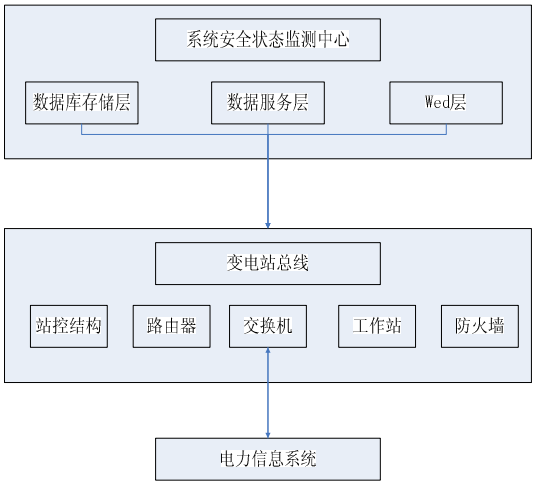

图 2 基于大数据分析的电力信息系统安全状态监测技术架构设计原理

3 技术大数据技术的电力信息系统安全状态监测方法

3.1 采集与存储安全状态数据

在基于大数据技术的电力信息系统安全状态监测方

法中，数据采集与存储是至关重要的第一步。为了确保数据的准确性和完整性，我们需要从各种来源收集电力信息系统的运行数据，包括但不限于发电、输电、配电和用电环节。这些数据可以包括实时数据、历史数据以及预测数据等[2]。数据采集过程中，需要采用安全可靠的数据采集设备和技术，以保证数据在采集过程中的安全性。同时，采集到的数据需要进行预处理，如数据清洗、去噪和格式转换等，以便于后续分析和处理。数据存储方面，应采用大规模分布式存储系统，如 Hadoop、Spark 等框架，以满足海量数据存储需求。同时，存储系统需要具备高可靠性、高性能和高可扩展性，以确保数据的安全性和稳定性。

3.2 确认电力信息系统安全数据关联性

在上述基础上，利用大数据技术，对电力信息系统中各安全要素的关联进行深入研究，为电力信息系统的运行状态监控提供理论基础。安全要素间存在着线性和非线性的复杂关系。在此背景下，利用大数据技术中的模糊等价关联分析方法，对网络安全要素间的关联进行研究。将安全状态数据采样集 G=(G_1G_2g)，而采样集相应的模糊子集合 H=(h_1，h_2h)，此处 h=（h_{x1}，$h_{x2}h$）,S=（1、2、r），r 是电力信息系统的安全状况的维数。由于模糊子集和原始采样集是非空集，因此，在两个集间存在着一种模糊关系，其表达方式见式（1）。

$$G\times H=\left\{(g,h)\middle|g\in,h\in H\right\} \quad (1)$$

针对电力信息系统的动态特性，为了确保数据的正确性，对以上两组数据进行了改进和计算，利用大数据技术，获得一组的修改程度 δ，其表达方式见式（2）。

$$\delta=\mu\left(\frac{GnH}{G}+\frac{GnH}{H}\right) \quad (2)$$

其中：μ 是电网安全状况信息的相关性系数，在相关性分析中，以相关系数 μ 为依据，对安全状况数据集进行改进，其等级划分的结果是：当相关性系数为（0,0.2）时，校正强度是 δ[3]。当相关系数取（0.005）时，校正强度是 0.5。当相关系数为 0。0,1 时，校正强度为 0。在此基础上，可得出电力信息系统安全状态数据之间所存有关联性。

3.3 基于神经网络算法的安全状态监测模型

在上述研究基础上，提出了一种基于神经网络的电力信息系统安全状态监控模型。在神经网络的输入层，将上述相关性分析所得之电力信息系统安全性信息，经由隐式层的运算，将初期的安全性监控结果输出。通过重复地训练，达到了数据信息的交互作用，从而获得了更精确的电力信息系统的安全性。模型计算过程如下。

如果将电力信息系统的安全性状况信息的信息矢量 A={a_1 a_2 ...a_r}，则根据时间而定的安全状况信息的信息向量 B（u）可以表达方式见式（3）。

$$B(u)=(b_1(u),b_2(u),...,b_r(u))$$
$$=u-(a_1(u),a_1(u-k)),...a_1(u-(r-1)k) \quad (3)$$

其中：u 是时刻，k 是一个滞后因子。该方法以电网安全状况资料的时序关系为输入级。将隐藏层的处理函数用 C（u）来描述，并在此基础上，将加权系数 m 作为隐藏层的基本准则，从而能够获得隐藏层的加权系数，其表达方式见式（4）：

$$C_q(u)=\frac{1}{1+e^{\gamma c\sum\varepsilon(u)mpq}} \quad (5)$$

其中：γ 是隐式结点的常量。对于安全状况资料，ε 是最优反应倾向。在对隐藏层进行多次重复的学习后，引进一个随机函数 N，从而获得了输出级的输出结果 D（u），其表示方式见式（6）。

$$D(a(u+1),N,B(u))=\frac{1}{\sqrt{a\pi v}}e^{\frac{(a(u+1)-v)^2}{2v^2}} \quad (6)$$

其中：v 是隐藏结点和相应权系数的相关关系。在此基础上，利用所建立的网络模型，对所建模型进行迭代训练，得到最优的电网安全监控结果。从而达到实时识别和监控电力信息系统的安全状况。在此基础上，提出了一种基于大数据的电力信息系统安全监控方案。

4 试验与检测

为验证本文所提出的大数据技术在电力信息系统中应用的可行性，本文设计了一套模拟仿真实验程序。以 Windows 为基础，构建测试平台，根据 M 电网企业的基础数据和组织结构，从测试系统 SQL Server 数据库中随机抽取 5 种攻击信号，并对其进行了分析，具体参数见表 1。

表 1 系统网络攻击信号参数

攻击信号种类	数量/组
IPsweep 攻击	100
Portsweep 攻击	100
Teardrop 攻击	100
Maibomb 攻击	100
Snopget 攻击	100

最后，利用 Matlab 编程，将系统攻击信号录入到表 1 中，比较了各种安全监控方式的效果。采用论文设计法（实验组）、传统（对照 1）、（对照 2）方法对所输入的数据信号进行识别和处理，从而获得该系统的安全状况监控结果，详情见图 3。在三种监控方式下，对各种类型的攻击信号，分别进行了测量，并对其进行了分析。

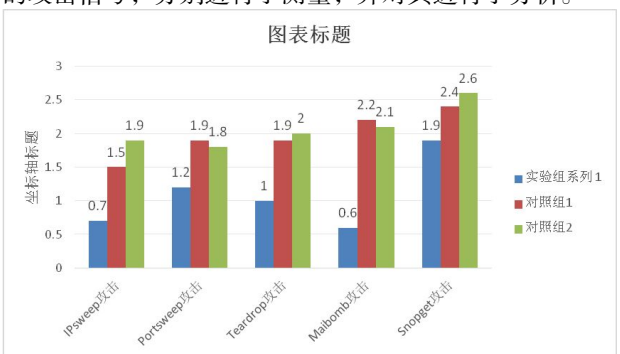

图 3 不同类型攻击信号辨识监测所用时间对比

从图 3 中可以看出，试验组识别和监控各种类型的攻击信号的时间比试验组 1 和试验组 2 要短，对于各种类型的攻击信号识别和监控所花费的时间平均为 0.944 秒。实验结果显示，本文所提出的方法能够快速地对监控信息进行处理，获得监控结果。基于以上分析，验证了该设计方法的可行性。在此基础上，将三种监控方式的监控数据进行对比，得出了三种监控方式对不同类型攻击信号识别监控精度的均值。从图 4 可以看出，对于各种类型的攻击信号，实验组的平均正确率都比控制组 1 和 2 高，对于各种攻击信号的监控正确率是 96.31%，比控制组 1 和 2 提高了 16.19%和 15.37%。通过本项目的研究，能够更加准确、及时地对系统中出现的安全隐患进行监控，为系统的维护和优化提供技术支持，从而提升电力系统的运行可靠性，保障电力工业的可持续可循环发展。

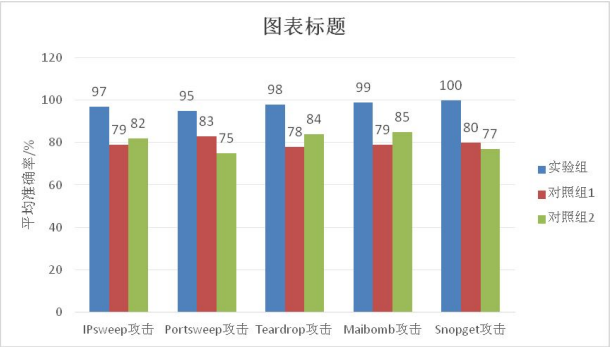

图 4 不同类型攻击信号辨识监测结果准确率对比

5 基于大数据技术的电力信息系统安全监测策略与建议

5.1 完善数据采集与传输机制

在基于大数据技术的电力信息系统安全监测中，首先需要完善数据采集与传输机制。这包括对电力系统各个环节的数据进行实时采集，确保数据的完整性和准确性。同时，采用加密和认证技术对数据传输过程进行保护，防止数据在传输过程中被窃取或篡改[4]。此外，还需建立健全的数据更新和维护制度，确保数据的实时性和可靠性。

5.2 提高数据存储与处理能力

为了满足基于大数据的电力信息系统安全监测需求，提高数据存储与处理能力是至关重要的。这涉及三个方面：一是扩大数据存储容量，确保大量数据的存储需求得以满足；二是提高数据处理速度，快速分析和处理海量数据，以实现实时监测；三是采用高效的数据挖掘和分析算法，从海量数据中提取有价值的信息，为安全监测提供有力支持。

5.3 构建智能安全监测体系

基于大数据技术的电力信息系统安全监测，需要构建一个智能化的安全监测体系。这一体系应包括以下几个方面：一是建立安全监测数据中心，实现数据的集中管理和分析；二是搭建智能监测平台，利用大数据技术实时收集和分析电力系统安全相关信息；三是运用人工智能算法，对监测数据进行智能分析，实现安全风险的自动识别和预警；四是建立完善的安全评估体系，对电力信息系统安全状态进行动态评估。

5.4 加强跨部门协同与沟通

在基于大数据技术的电力信息系统安全监测中，加强跨部门协同与沟通至关重要。各部门之间需要建立健全的信息共享机制，确保安全监测数据的及时、准确传递。此外，加强内部培训和外部合作，提高员工对大数据技术在电力信息系统安全监测中的应用认识，提升整体监测水平[5]。

5.5 制定相应的安全防护规范与措施

为确保基于大数据技术的电力信息系统安全监测的有效实施，需要制定相应的安全防护规范与措施。包括以下几个方面：一是制定数据采集、存储、处理和分析的相关规范，确保数据安全；二是建立完善的安全管理制度，明确各部门安全职责和权限；三是针对大数据特点，制定针对性的安全防护策略，如加强数据加密、提高网络安全防护等；四是开展定期安全检查和评估，及时发现并整改安全隐患；五是制定应急预案，确保在发生安全事件时能够迅速应对。

结语：

随着我国电力物联网的快速发展，电网的信息化程度不断提高，而电力信息系统则是构建智能电网、协调发电、输电和配电的重要环节。整个电力信息系统，包括变、用等，都能有效、稳定地运行。目前，大部分电力信息系统的安全性研究主要集中在安全防护与检测方面，而在智能电网中，安全态势感知仍是一个悬而未决的难题。但实际上，很多安全隐患都是在很短的一段时间里才会出现，而且都是由防护与探测元件的撤出所控制的。这种危险往往会给电网带来很大的冲击，而当它们被发现，再想采取措施进行防御时，往往为时已晚，造成破坏也是很难估算的。本项目以电网安全态势感知为研究对象，采用基于模糊聚类的关联分析、博弈论、增强学习等机器学习方法，建立基于大数据的电网安全态势感知模型。通过模拟与试验，验证了所提出的监控模型的正确性与正确性，为提高智慧网格的安全水平提供了理论依据。

参考文献：

[1]王国峰,唐云善,徐立飞.电力信息系统软件代码漏洞检测系统的设计与实现[J].微型电脑应用,2023,39(11):118-121.

[2]张向聪,张潺,杨莹等.智能信息系统业务事件驱动机理分析与运维模型优化研究[J].粘接,2023,50(10):181-184.

[3]王扶文，肖建军，刘国亮等.基于 CNN+C5.0 的电力信息系统网络入侵检测模型[J].电力大数据,2022,25(08):37-44.

[4]陈明,张凯,王熙等.基于大数据的电力信息系统网络安全路径探索[J].科技资讯,2022,20(15):47-49.

[5]郭永和,闫龙川,白东霞等.面向电力信息系统的分布式自动化测试集成平台[J].网络安全技术与应用,2022,(07):103-106.