基于数据挖掘的电力系统网络安全漏洞识别方法探讨

邓　昊
山东鲁软数字科技有限公司　山东济南　250100

摘　要：随着电力系统数字化、智能化转型加速，其面临的网络安全威胁日益严峻。传统基于规则库和签名的防御手段难以应对新型、未知攻击。本文分析了电力系统网络安全核心特性，指出目前电力系统网络安全现状，阐述了电力系统网络安全评估框架和标准，提出数据挖掘在电力系统网络安全漏洞识别中的具体应用，希望为构建电力系统网络安全主动防御体系提供新思路。

关键词：数据挖掘；电力系统；网络安全；漏洞；识别

前言

电力系统作为国家关键信息基础设施的核心组成部分，其网络安全直接关系国民经济命脉与社会稳定。随着智能电网建设的加速推进，SCADA系统、智能电表、分布式能源控制器等大量终端设备接入网络，在提升系统智能化水平的同时，也显著扩大了攻击面。近年来，针对电力系统的APT攻击、勒索病毒、零日漏洞利用等高级威胁事件频发，暴露出传统安全防护体系的严重不足。数据挖掘技术通过从海量异构数据中提取潜在规律，为破解上述难题提供了新路径。

一、电力系统网络安全核心特性解析

（一）架构复杂，OT/IT深度融合的攻防矛盾

电力系统作为典型的信息物理融合系统，其网络架构呈现三层异构融合特征。过程层部署传感器与执行器，采用IEC 61850-9-2、GOOSE/SV等协议进行实时控制。这些协议采用无认证广播通信机制，攻击者可通过ARP欺骗伪造智能终端身份。间隔层的继电保护装置和远程终端单元依赖Modbus TCP、DNP3.0等工控协议。这些协议普遍采用明文传输，存在漏洞，攻击者发送畸形功能码即可篡改断路器状态参数。站控层的SCADA系统与HMI人机接口通过IEC 60870-5-104、OPC UA协议交互，高危端口暴露问题突出。架构复杂导致电力系统网络安全存在网络刚性约束与安全动态需求的冲突。工业PLC等设备要求10万小时以上的平均无故障时间，无法频繁升级补丁，而电力系统网络安全需实时应对网络漏洞。这种矛盾导致防护策略难以同步更新，形成安全洼地。

（二）要求实时性约束下技术瓶颈

电力业务的实时性要求对安全检测构成严苛限制。例如，现有的继电保护业务允许最大延迟仅4ms，数据采样周期达微秒级（1-2μs），要求安全检测在1ms内完成响应。传统深度学习模型推理延迟超过200ms，完全无法满足需求。在数据运算能力上，目前电力系统同步相量测量装置等智能终端仅配备512MB内存，无法运行完整入侵检测引擎。

（三）工业控制通信设备存在先天缺陷

主流电力工控协议存在系统性安全缺陷。现有的Modbus TCP完全缺乏认证与加密机制，攻击者可直接发送功能码篡改设备参数。实际攻击中，黑客常组合使用功能码读线圈状态和写单个线圈实现侦察与破坏。在弱口令认证上，70%存量设备不支持TLS 1.3加密，导致CVE-2020-15780等应用服务数据单元注入漏洞广泛存在，攻击者可伪造遥测数据触发误判。目前DNP3.0协议因无报文完整性校验，易遭受畸形报文拒绝服务攻击，引发主站通信中断。更危险的是协议语义隐蔽性——符合规范的GOOSE重放报文可被用于延迟保护动作，规避规则库检测。

（四）网络数据治理面临数据多元化挑战

安全分析依赖的四类核心数据面临治理难题：网络流数据日增量达10TB，需实时处理50+维特征；系统日志呈非结构化特征（如SCADA操作记录），需定制正则表达式解析；设备状态快照具有强时序相关性，但不同

作者简介：邓昊（1982.07-），男，汉族，山东济南人，学士，工程师，研究方向：人工智能或其他。

系统存在毫秒级时间漂移；用户操作审计需结合领域知识定义特征（如“五分钟内连续切换保护定值区”）。目前电力系统网络监控对于用户的数据安全防护，要求数据不出生产控制大区，限制云端协同分析，无法对海量电力数据进行后台分析，数据治理面临多元化挑战。

二、当前电力系统网络安全现状分析

（一）基础设施脆弱性凸显

现有电力系统网络安全中，存量设备成为主要高危漏洞。全国超60%在运继电保护装置使用未打补丁的VxWorks 5.5系统，平均服役年限达12年，无法热升级。省级调度中心核心交换机中，32%存在未修复的SNMP协议漏洞，可导致网络拓扑泄露。在基础设施中，工控协议原生缺陷，导致成为网络安全漏洞的主要原因。Modbus TCP协议在县级电网覆盖率超85%，但缺乏加密认证机制。此外，目前智能电表、光伏逆变器等海量终端直连调度云平台，攻击面扩大，导致电力系统容易受到多种来源网络攻击，某地调系统因OA服务器漏洞，被植入恶意软件横向穿透隔离网闸。

（二）新型攻击威胁升级

在电力系统网络安全中，针对电网黑客组织攻击具有持续性与针对性。在攻击手法上，国家级黑客组织采用鱼叉邮件+0day漏洞（的攻击方式，在攻击目标上，倾向于能量管理系统与广域测量系统，且利用植入病毒的方式，病毒潜伏期长达一年。在针对电力系统网络安全攻击中，病毒勒索已经形成产业化。新型勒索软件具备PLC锁屏能力，某发电厂2022年因控制系统被加密导致停机8小时。此外，新型攻击技术涌现，通过篡改SCADA系统地理信息数据，引发潮流计算错误，或者针对智能变电站光纤通道，用特定波长激光干扰采样值（SV）报文，成功率超70%，严重影响着电力系统网络安全。

（三）防御体系存在结构性短板

目前，电力企业对于网络安全防御存在技术能力不足的问题。根据中国电科院测试，目前入侵检测系统对工控协议识别率仅62%，无法解析IEC 104 ASDU嵌套结构。省级电网日均告警量超50万条，但有效分析率＜5%，误报率高达85%。在管理机制上，目前对生产控制系统补丁平均部署周期达143天，高危漏洞修复存在不及时的问题。《电力监控系统安全防护规定》要求“生产控制大区禁止无线通信”，但5G差动保护试点被迫违规部署，现有管理制度无法与实际部署相一致。

（四）数据安全风险剧增

在电力系统网络安全管理中，敏感数据泄露成为数据安全的主要因素。现有的电力系统数据传输中，调度指令、机组出力计划等核心数据明文传输占比达45%，在目前的网络环境下，容易引发核心电网数据泄露。例如，某新能源集控中心数据库暴露公网，导致17个风电场运行参数被窃取。在数据治理上，多源数据时标偏差，SCADA与PMU数据时间差最大达200ms，影响攻击关联分析。此外，现有电网用户隐私保护缺失，用户用电行为数据未脱敏直接用于负荷预测，违反《个人信息保护法》。

三、电力系统网络安全评估框架和标准

（一）评估框架核心架构

国内电力网络安全评估采用“三纵四横”立体模型，以《电力监控系统安全防护规定》（国能安全〔2015〕36号文）为纲领。在纵向深度防御中，调度端，省级以上调度中心需部署入侵检测系统（IDS）与安全信息事件管理平台（SIEM），实时关联分析跨区告警；厂站端，变电站/发电厂控制区部署硬件防火墙，禁止非授权设备接入生产控制大区；终端，智能电表、PMU等终端设备强制启用安全启动与固件签名验证。在横向区域隔离中，可以分为生产控制大区与管理信息大区两部分。生产控制大区又分为安全Ⅰ区、Ⅱ区。Ⅰ区实时控制业务与Ⅱ区非实时业务间采用逻辑隔离，Ⅱ区与Ⅲ区部署单向隔离装置（光闸），传输延迟须＜1ms。管理信息大区，互联网接入区（Ⅳ区）邮件系统与Ⅲ区间部署双向认证网关，阻断OPC UA等协议穿透

（二）电力系统网络安全核心标准体系

我国现有电力系统网络安全核心标准体系主要由：《信息安全技术网络安全等级保护基本要求》、《电力监控系统安全防护方案》、行业技术规范三部分构成。《信息安全技术网络安全等级保护基本要求》主要包括物理环境、通信网络、区域边界三部分，对电力系统软件与硬件安全防护做出明确要求。《电力监控系统安全防护方案》则要求采用加密认证，纵向加密装置采用国密SM4算法，调度证书体系基于SM2椭圆曲线，密钥更新周期≤90天。要求安全审计中，操作日志留存≥180天，关键行为需同步录屏并关联操作员指纹信息。行业技术规范主要包括《智能变电站网络安全验收规范》、《电力行业网络安全红蓝对抗指南》，对电力系统网络安全提出具体操作要求。

（三）电力系统网络安全评估实施方法

电力系统网络安全评估实施方法主要包括：静态合规核查、动态渗透测试、运行态风险评估三种。静态合规核查是对设备基线检查，通过安全内容自动化协议脚本自动核查，利用防火墙策略是否关闭对高危端口进行检查。察看操作系统补丁版本是否符合《电力行业漏洞修复目录》要求。动态渗透测试是对电力系统网络进行模拟攻击，模拟发送异常ASDU报文，检测监控系统是否发生雪崩崩溃，构造Modbus功能码，验证保护装置是否触发异常告警。运行态风险评估是对业务连续性分析，量化攻击对电力业务的影响。

四、数据挖掘在电力系统网络安全漏洞识别中的具体应用

（一）实现网络安全漏洞精准识别

传统电力安全防护依赖人工设定规则，对于网络安全漏洞局限于发生问题后进行漏洞追踪，无法实现事前预防，而数据挖掘技术则提前对电力系统网络数据进行深度扫描与分析，从海量运行数据中自动发现异常线索。数据挖掘能够实现全天候扫描，持续分析网络流量、设备日志、用户操作记录等多元信息，覆盖调度中心、变电站、智能电表等各个环节。对于异常行为，数据挖掘通过比对历史正常状态，自动识别偏离常规的模式。例如某台设备突然在深夜频繁发送指令，或某个账号尝试访问从未操作过的系统区域。此外，数据挖掘还能发现隐藏漏洞，对于缺乏关联的网络完全问题进行追踪，分析其背后运行逻辑，实现对网络安全漏洞的精准识别。

（二）多维度数据分析应用

数据挖掘在网络安全漏洞识别上，能够从多个维度分析电网数据，主要应用在网络深体检、设备日志智能解读、用户行为模式识别三方面。网络深度体检上，数据挖掘下的网络安全漏洞识别，能够自动识别异常通信，当某个智能电表在1分钟内向控制中心发送上千次数据，系统会标记为“疑似拒绝服务攻击”。当发现伪装成正常工控协议的恶意指令。例如攻击者将非法操作隐藏在合法的电力通信协议格式中，数据挖掘能通过分析指令组合规律识破伪装。在设备日志智能解读上，对故障原因进行关联性分析，从而结合电网异常波动，检测设备产生故障原因。在权限管理上，能够监测账号异常执行，确保账号安全。用户行为模式识别中，基于深度挖掘，能够建立操作人员“数字指纹”，通过分析历史操作习惯，当检测到异常行为，自动触发二次验证。

（三）建立预测性防护

基于数据挖掘的电力系统网络安全漏洞识别，应建立预测性防护，对漏洞进行早期预警。基于设备运行状态预测风险，当某类继电保护装置连续出现内存异常占用，结合其固件版本信息，可预判存在未公开漏洞。在网络漏洞识别上，分析攻击路径，分析黑客的试探性动作，自动模拟后续攻击步骤，提前加固薄弱环节。此外，还要建立自适应防御机制，当发现新型攻击模式，自动生成检测规则并下发到相关设备。随着人工智能技术的发展，还可以通过持续学习，区分真实攻击与正常业务波动，提升网络安全漏洞防护质量。

总结

随着信息技术的发展，利用数据挖掘对电力系统网络安全进行识别，能够有效破解目前电力系统网络安全频发的问题。数据挖掘技术将电力安全从“事后补救”转向“事前预防”，从“单点布防”升级为“全局免疫”，为构建本质安全的新型电力系统提供核心支撑。守护电网安全，就是守护每盏灯背后的万家灯火。

参考文献

[1]高翔，陈贵凤，赵宏雷.基于数据挖掘的电力信息系统网络安全态势评估[J].电测与仪表，2019，56（19）：102-106.

[2]王燕.基于数据挖掘的电力通信网络安全态势识别系统设计[J].通信电源技术，2024，41（16）：7-9.

[3]王婧怡，张熙昊，朱莹.基于数据挖掘的电力信息系统网络安全态势评估[J].2024（15）：151-153.

[4]吕国曙，鞠磊.基于数据挖掘的电力系统网络安全漏洞识别方法[J].电工技术，2023（2）：49-51.