Smart Grid 智能电网, 2026, 16(4), 106-112
Published Online August 2026 in Hans. https://www.hanspub.org/journal/sg
https://doi.org/10.12677/sg.2026.164013

Hans汉斯

基于人工智能动态优化的配电网网络安全风险评估方法研究

高雅婷[1]，刘俊文[1]，李伟良[1]，王　婵[1]，张哲宁[1]，林冰洁[1]，陶学通[2*]

[1]国家电网有限公司信息通信中心，网络与数据安全部，北京
[2]杭州电子科技大学管理学院，浙江　杭州

收稿日期：2026年7月13日；录用日期：2026年8月5日；发布日期：2026年8月17日

摘　要

随着智能配电网建设不断推进，配电网运行过程逐渐依赖环境传感器、相量测量单元、智能电表、电力线路传感器、SCADA监测系统以及通信接口等多源数据进行状态感知、运行分析和控制决策。与此同时，虚假数据注入、异常网络流量、恶意数据模式以及针对智能控制过程的攻击行为，可能影响配电网基础设施的安全运行和决策结果的可靠性。针对现有网络安全风险评估方法实时性不足、多源数据利用不充分以及风险结果难以支撑运行控制等问题，本文提出一种基于人工智能动态优化的配电网网络安全风险评估方法。该方法首先采集原始电力负荷、环境数据、设备工作状态、发电侧数据、供电侧信息、组件温度、网络状态以及网络安全风险因素等数据；其次对多源数据进行汇聚、清洗、标准化和特征提取，形成标准化安全评估输入；然后结合入侵检测、威胁建模、风险因素不确定性度量和安全阈值判断，实现对网络安全风险的动态评估；最后将风险评估结果输入决策支持系统，形成安全警报、风险缓解策略或控制信号。仿真分析表明，该方法能够将网络安全风险识别结果与实时网格优化、运行状态反馈和决策控制过程相结合，为智能配电网的安全运行和韧性提升提供支撑。

关键词

智能配电网，网络安全，风险评估，人工智能，动态优化，决策支持

Research on Cybersecurity Risk Assessment Method for Distribution Networks Based on Artificial Intelligence Dynamic Optimization

Yating Gao[1], Junwen Liu[1], Weiliang Li[1], Chan Wang[1], Zhening Zhang[1], Bingjie Lin[1], Xuetong Tao[2*]

[1]Department of Cyberspace and Data Security, Information & Telecommunication Center-State Grid Corporation of China, Beijing

[*]通讯作者 Email: 3193393069@qq.com

文章引用: 高雅婷, 刘俊文, 李伟良, 王婵, 张哲宁, 林冰洁, 陶学通. 基于人工智能动态优化的配电网网络安全风险评估方法研究[J]. 智能电网, 2026, 16(4): 106-112. DOI: 10.12677/sg.2026.164013

[2]School of Management, Hangzhou University of Electronic Science and Technology, Hangzhou Zhejiang

Received: July 13, 2026; accepted: August 5, 2026; published: August 17, 2026

Abstract

With the development of smart distribution networks, operational monitoring and control increasingly rely on multi-source data collected from environmental sensors, phasor measurement units, smart meters, power line sensors, SCADA systems and communication interfaces. Meanwhile, false data injection, abnormal network traffic, malicious data patterns and attacks against intelligent control processes may affect secure operation and decision reliability. To address insufficient real-time performance, inadequate utilization of multi-source data and weak support of risk assessment results for operation control, this paper proposes a cybersecurity risk assessment method for distribution networks based on artificial intelligence dynamic optimization. Multi-source operational and security data are collected, aggregated, cleaned, normalized and extracted to form standardized security assessment inputs. Intrusion detection, threat modeling, uncertainty measurement of risk factors and security threshold judgment are then combined to achieve dynamic cybersecurity risk assessment. Finally, the assessment results are sent to the decision support system to generate security alerts, risk mitigation strategies or control signals. The analysis shows that the proposed method can integrate cybersecurity risk identification with real-time grid optimization, operational feedback and decision control, thereby supporting secure operation and resilience improvement of smart distribution networks.

Keywords

Smart Distribution Network, Cybersecurity, Risk Assessment, Artificial Intelligence, Dynamic Optimization, Decision Support

1. 引言

智能配电网通过传感器、智能电表、通信接口、边缘计算和云计算等技术实现对电力系统运行状态的实时感知和动态控制。与传统配电网相比，智能配电网在提升运行效率、增强供电可靠性和支撑需求响应方面具有明显优势。然而，随着信息通信技术与电力基础设施的深度融合，配电网运行过程也面临更加复杂的网络安全威胁。攻击者可能通过虚假数据注入、通信链路干扰、恶意数据篡改等方式影响电网状态感知和控制决策，进而造成运行效率下降、风险响应延迟甚至局部运行失稳[1]。

现有配电网安全防护方法多侧重于单点警报或静态规则判断，难以适应智能配电网中多源数据并行接入、网络状态快速变化和运行控制实时联动的应用场景[2]。尤其在需求响应、实时网格优化和智能控制协同运行过程中，网络安全风险不再只是单一通信异常问题，而是可能与负荷分布、电压波动、设备性能、电网性能反馈和控制信号生成过程相互耦合。参考文献[3]提出的人工智能动态网格优化分析方法表明，将实时数据分析、预测性维护和网络安全风险评估相结合，有助于提升智能配电网运行韧性。

本文基于人工智能动态优化思想，提出一种面向配电网的网络安全风险评估方法。该方法以多源数据采集和预处理为基础，以入侵检测、威胁建模、风险因素不确定性度量和风险修正计算关系为核心，

以决策支持系统和安全警报响应过程为输出支撑，形成“数据输入－数据处理－风险评估－决策支持－结果输出”的技术流程。

2. 配电网网络安全风险评估总体框架

本文所提出的方法包括数据采集与预处理、网络安全风险评估结构构建、威胁检测与风险评估、风险结果输出与应用四个环节。

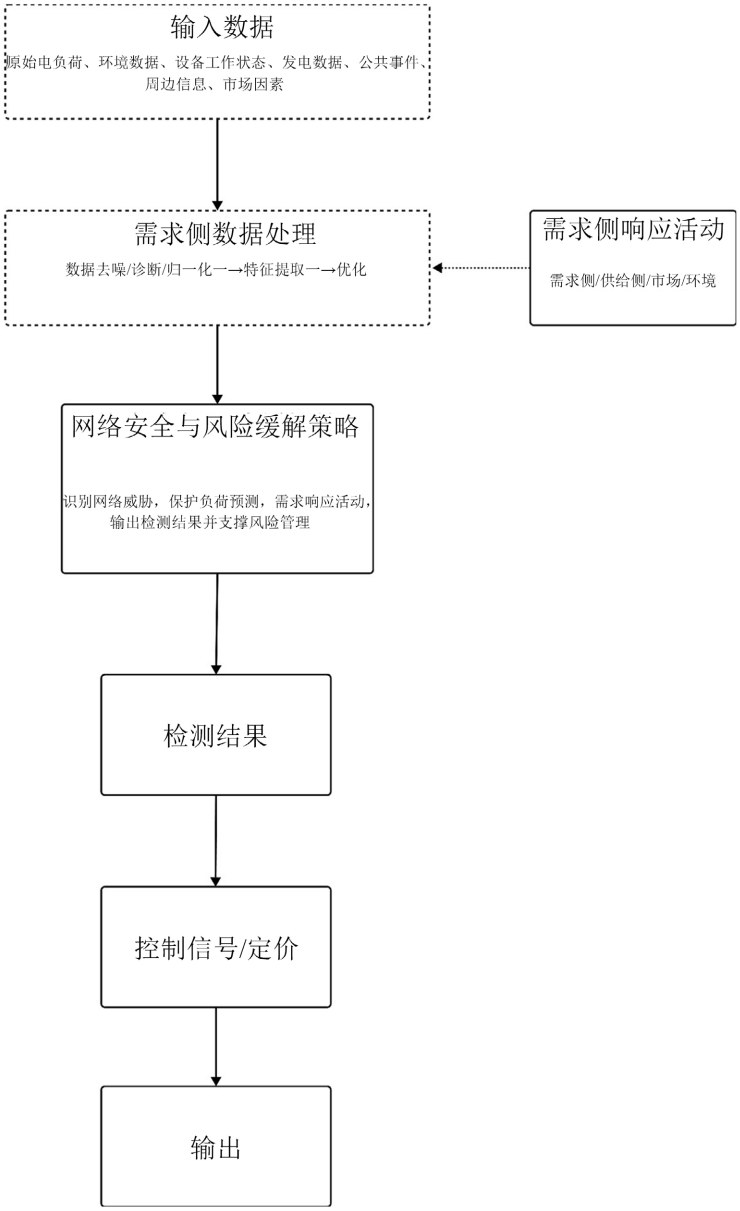

Figure 1. Demand-side cybersecurity and risk mitigation process
图 1. 需求侧网络安全与风险缓解流程图

在数据输入环节，配电网通过环境传感器、相量测量单元 PMU、IoT 设备、智能电表、电力线路传感器、SCADA 监测系统、通信接口以及网络状态监测设备等获得运行数据和安全相关数据。采集内容包

括原始电力负荷、环境数据、设备工作状态、发电侧数据、供电侧信息、组件温度、网络状态和网络安全风险因素等。其中，网络安全风险因素数据并非由单一硬件直接产生，而是由通信接口日志、SCADA 监测记录、网络状态监测结果、入侵检测结果、威胁建模结果和安全警报响应记录共同形成，用于表征异常网络行为、恶意数据模式、虚假数据注入风险和网络状态异常。

在数据处理环节，首先对不同来源的数据进行汇聚和排序，形成连续数据流；其次对缺失数据、异常噪声和无效记录进行清洗；再次对不同量纲的数据进行标准化处理；最后从清洗后的数据中提取能够反映配电网运行状态和网络安全状态的关键特征，形成标准化安全评估输入数据。该处理过程对应图 1 中的数据去噪、诊断、归一化、特征提取和优化环节。

在风险评估环节，标准化安全评估输入数据进入实时网络安全风险评估层。该层结合入侵检测系统、威胁建模方法、风险因素不确定性计算关系和安全风险阈值，对异常网络行为、异常数据流、恶意数据模式和网络状态异常进行识别，并生成风险评估结果[4]。

在结果输出环节，风险评估结果进入决策支持系统。决策支持系统根据风险评估率、风险因素不确定性、威胁检测结果、风险修正结果和控制信号，生成安全警报、风险缓解策略或运行控制建议[5]。该过程不仅服务于网络安全防护，也可与负荷分布、电网稳定性、功率使用、电压波动、设备性能和电网性能反馈等实时网格优化结果相结合，从而提高配电网运行韧性。网络安全分层架构如图 2 所示。

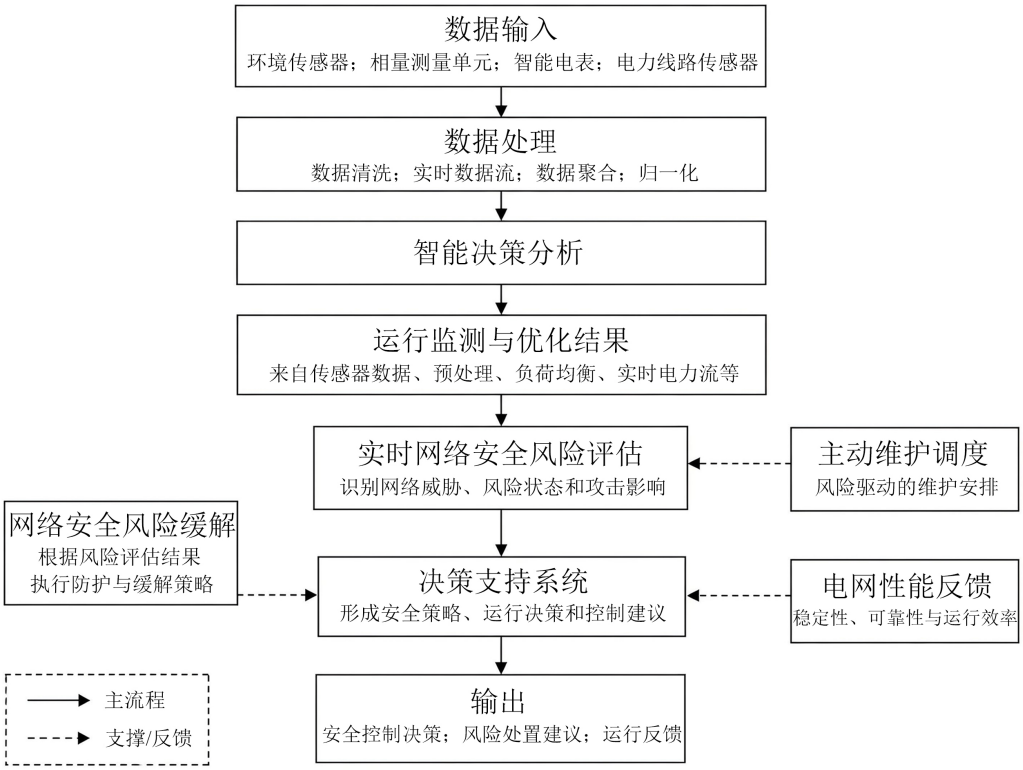

Figure 2. Layered architecture for cybersecurity risk assessment
图 2. 网络安全分层架构图

3. 多源数据输入与预处理方法

配电网网络安全风险评估需要同时考虑运行侧数据和网络侧数据。本文将数据来源划分为运行数据、环境数据、设备状态数据、通信网络数据和安全风险数据五类。运行数据包括原始电力负荷、供电侧信

息和发电侧数据；环境数据包括环境传感器数据、温度、湿度、天气等环境状态数据；设备状态数据包括设备工作状态、组件温度和电力线路传感器数据；通信网络数据包括通信接口数据、网络状态监测数据和通信链路状态[6]；安全风险数据包括异常数据记录、入侵检测结果、威胁建模结果和安全警报响应记录。各类数据来源及其在本文方法中的含义如表 1 所示。

Table 1. Data sources and definitions for cybersecurity risk assessment in distribution networks
表 1. 配电网网络安全风险评估数据来源与定义

类别	数据来源或数据类型	在本文方法中的含义
运行数据	原始电力负荷、供电侧信息、发电侧数据	用于反映配电网实时运行状态和供需变化
环境数据	环境传感器数据、温度、湿度、天气等环境状态数据	用于反映外部环境扰动，为需求侧分析、运行状态判断和风险评估提供背景
设备状态数据	设备工作状态、组件温度、电力线路传感器数据	用于判断设备运行状态与安全风险之间的关联
通信网络数据	通信接口数据、网络状态监测数据、通信链路状态	用于识别通信异常、数据传输异常和网络状态变化
安全风险数据	入侵检测结果、威胁建模结果、安全警报响应记录	用于表征网络安全风险因素和异常行为模式

数据预处理过程包括数据汇聚、数据清洗、标准化处理和特征提取。数据汇聚用于将多源异构数据统一组织为连续数据流；数据清洗用于降低异常噪声、缺失记录和无效数据对风险评估的影响；标准化处理用于消除不同量纲之间的差异；特征提取用于从运行状态、网络状态和安全风险因素中提取能够表征安全状态的关键变量。经过上述处理后，可形成标准化安全评估输入数据，为后续风险评估结构构建和风险计算提供基础。

4. 网络安全风险评估方法

设时刻 n 的标准化安全评估输入数据为 $X(n)$，则可表示为：

$$X(n)=\{L(n),E(n),S(n),N(n),Z(n)\} \tag{1}$$

其中，$L(n)$ 表示负荷及供电侧相关数据，$E(n)$ 表示环境数据，$S(n)$ 表示设备工作状态和组件温度，$N(n)$ 表示网络状态数据，$Z(n)$ 表示网络安全风险因素数据。环境数据 $E(n)$ 来源于环境传感器和运行监测记录，主要用于反映温度、湿度、天气等外部环境状态对需求侧响应、运行状态判断和风险评估的影响。

为判断网络安全风险评估结果是否满足最低有效判断条件，设 $R(x)$ 为随时间 x 变化的网络安全风险评估率，R_{mn} 为系统设定的最小风险阈值，则有：

$$R(x)\geq R_{mn} \tag{2}$$

当 $R(x)$ 满足阈值要求时，说明当前数据和风险评估结果能够支撑后续决策；当 $R(x)$ 低于阈值时，需要提高采样频率、补充数据来源或触发进一步分析。

为了度量网络安全风险因素的不确定性，可引入信息熵思想，对网络状态、运行状态和风险因素之间的不确定性关系进行描述：

$$-M_v(n-1)=H(e,w)-H(z),Q>R(n-f) \tag{3}$$

其中，$H(z)$ 表示网络安全风险因素的不确定性或熵，$H(e,w)$ 表示网络状态和运行状态的不确定性，$M_v(n-1)$ 表示上一时刻评估性能，$Q>R(n-f)$ 表示风险评估满足最低有效判断条件。该式用于描述风险因素不确定性对安全风险评估结果的影响。

综合考虑风险因素变化和风险评估输出结果，可采用如下风险修正形式：

$$M_q^{w-1}(yz) \coloneqq \left[m(z-p) + Z\left(mk - E_r^{n-1}\right) \right] Z_y^{p-1} \tag{4}$$

其中，$m(z-p)$表示风险因素变化对评估结果的影响，$Z\left(mk - E_r^{n-1}\right)$表示修正后的评估性能量，$Z_y^{p-1}$表示时间尺度下的归一化因子。该式用于表示风险评估结果随实时数据变化而调整。

最终，安全决策输出可表示为：

$$D(n) = f\left(Q, M_v(n-1), M_\varphi^{w-1}(yz), J(n-1), K|m|^{r-(b-ser)}\right) \tag{5}$$

其中，$D(n)$表示当前时刻的安全决策输出，$f(\cdot)$表示决策函数，$J(n-1)$表示上一时刻初始评估状态，$K|m|^{r-(b-ser)}$表示网络安全韧性和风险调节影响。通过该决策输出，可将实时风险评估结果转换为安全警报、风险缓解策略或控制信号。

5. 实验设计与结果分析

为验证本文方法的有效性，可采用四节点星型配电网络作为测试场景。该场景包括一个供电节点和三个用户节点，初始数据集包含 10,000 组观测样本，扩展后形成 60,000 组观测样本，包含 12 个核心特征和 2 个因变量。实验数据包括原始电力负荷、环境数据、设备工作状态、组件温度、网络状态、安全风险因素等。

实验过程包括以下步骤：首先采集多源运行数据和网络安全相关数据；其次对数据进行清洗、排序、标准化和特征提取；然后利用入侵检测步骤识别异常网络行为和异常数据模式；再通过威胁建模步骤分析潜在威胁场景和风险关系；最后基于风险评估率、风险因素不确定性和风险修正计算关系生成风险评估结果，并将其输入决策支持系统。根据仿真结果，可整理得到表 2 所示的性能结果示例。

Table 2. Example of simulation performance analysis results
表 2. 仿真性能分析结果示例

结果指标	结果值	对应含义
网络安全威胁检测分析	94.8%	反映入侵检测与威胁建模对网络安全风险识别的有效性
实时网格优化分析	96.5%	反映运行状态反馈对风险决策的支撑效果
可扩展性分析	95.1%	反映多节点、多源数据场景下方法的适应能力
成本分析	19%	反映风险评估与运行优化对成本控制的支撑作用
准确率	98.9%	反映风险评估结果整体正确性
精确率	97.1%	反映被识别为风险样本中的有效识别比例
召回率	96.5%	反映真实风险样本被检测出的覆盖程度
F1 值	97.4%	综合反映精确率和召回率之间的平衡效果

从表 2 可以看出，基于人工智能动态优化的风险评估方法能够在网络安全威胁检测、实时网格优化和风险识别准确性方面取得较好效果。尤其是在多源数据输入和动态风险修正机制的支撑下，该方法能够将网络安全风险识别结果与配电网运行状态、控制信号和决策支持过程进行关联，从而提升配电网安全风险评估的实时性和可解释性。

6. 讨论

本文方法的优势主要体现在以下三个方面。第一，数据来源更加全面。方法同时考虑运行数据、环

境数据、设备状态数据、通信网络数据和安全风险数据，能够更全面地描述配电网运行与网络安全状态。第二，风险评估过程具有动态性。通过风险因素不确定性度量和风险修正计算关系，评估结果可以随实时数据流和网络状态变化进行调整。第三，评估结果能够服务于决策控制。该方法不仅输出风险识别结果，还将风险评估率、风险修正结果、控制信号和电网性能反馈输入决策支持系统，使网络安全防护与运行优化过程相结合。

需要指出的是，本文方法仍存在进一步完善空间。首先，网络安全风险因素的提取依赖多源数据质量，当通信链路数据不完整或传感器数据存在大规模缺失时，可能影响风险评估结果的稳定性。其次，威胁建模过程需要结合更多真实攻击样本，以提升对复杂攻击场景的泛化能力。最后，风险评估结果与实际控制策略之间的映射关系仍需在更复杂的配电网场景中进一步验证。

7. 结论

本文提出了一种基于人工智能动态优化的配电网网络安全风险评估方法。该方法以多源数据采集和预处理为基础，融合入侵检测、威胁建模、风险因素不确定性度量和风险修正计算关系，实现了对配电网网络安全风险的动态评估。通过引入环境数据、设备状态数据、网络状态数据和安全风险数据，方法能够更全面地反映智能配电网运行过程中的安全状态变化。仿真结果表明，该方法在网络安全威胁检测、实时网格优化、准确率、精确率、召回率和 F1 值等方面具有较好的表现，可为智能配电网安全运行、风险缓解和决策支持提供技术支撑。

后续研究可进一步结合真实配电网运行数据和攻击样本，对风险评估结构、威胁建模过程和决策输出机制进行优化，以提升方法在复杂场景下的实用性和推广价值。

参考文献

[1] Liu, Y., Ning, P. and Reiter, M.K. (2011) False Data Injection Attacks against State Estimation in Electric Power Grids. *ACM Transactions on Information and System Security*, **14**, 1-33. https://doi.org/10.1145/1952982.1952995

[2] Mo, Y.L., Kim, T.H., Brancik, K., Dickinson, D., Lee, H., Perrig, A., *et al*. (2012) Cyber-Physical Security of a Smart Grid Infrastructure. *Proceedings of the IEEE*, **100**, 195-209. https://doi.org/10.1109/jproc.2011.2161428

[3] Ashraf, M.W.A., Avanija, J., Ballireddy, T.R.R., Singh, A.R., Bajaj, M. and Rubanenko, O. (2025) Artificial Intelligence-Driven Dynamic Optimization for Predictive Maintenance and Cybersecurity in Smart Power Distribution Networks. *Energy Exploration & Exploitation*, **44**, 771-798. https://doi.org/10.1177/01445987251386897

[4] Gunduz, M.Z. and Das, R. (2020) Cyber-Security on Smart Grid: Threats and Potential Solutions. *Computer Networks*, **169**, Article 107094. https://doi.org/10.1016/j.comnet.2019.107094

[5] Pillitteri, V.Y. and Brewer, T.L. (2014) Guidelines for Smart Grid Cybersecurity. NISTIR 7628 Revision 1, National Institute of Standards and Technology.

[6] International Electrotechnical Commission (2023) IEC 62351: Power Systems Management and Associated Information Exchange-Data and Communications Security. International Electrotechnical Commission.