 DOI: https://doi.org/10.12345/bdai.v6i2.24578

Research on the intelligent detection system design of power distribution center

Qiuying Weng Li Luo Jianbin Cheng Yifang Wei Hui Yang

Quzhou Jiaoyang New Energy Technology Co., Ltd., Quzhou, Zhejiang, 324000, China

Abstract

This study aims to develop an intelligent detection system of power distribution center based on Internet of Things technology to realize real-time detection of abnormal intrusion and intelligent monitoring of environmental parameters.The system design includes database architecture, system framework construction, illegal intrusion algorithm and environmental parameter monitoring algorithm optimization and so on.Through detailed system requirements analysis, the functional requirements and performance indicators are defined, and the system adopts advanced sensor technology and data analysis algorithm to ensure efficient data acquisition, processing and transmission.

Keywords

power distribution center; intelligent detection; system design

配电中心智能检测系统设计研究

翁秋英 罗丽 程建彬 魏一芳 杨惠

衢州骄阳新能源科技有限公司，中国·浙江 衢州 324000

摘 要

本研究旨在开发一款基于物联网技术的配电中心智能检测系统，以实现对人员非正常入侵的实时检测和环境参数的智能监测。系统设计包括数据库架构、系统框架搭建、非法入侵算法及环境参数监测算法优化等多个方面。通过详细的系统需求分析，明确了功能需求和性能指标，系统采用先进的传感器技术和数据分析算法，确保高效的数据采集、处理与传输。

关键词

配电中心；智能检测；系统设计

1 引言

配电中心作为电力供应的核心，其稳定性和安全性至关重要。本研究开发基于物联网的配电中心智能检测系统，集成传感器技术和数据分析算法，实现环境参数实时监测和人员入侵及时预警。

2 系统需求分析

2.1 功能需求

为了满足配电中心智能化管理的需求，系统必须具备若干关键功能。系统需要实现对人员非正常入侵的实时检测。这意味着在任何未经授权的人员进入配电中心时，系统能够立即识别并发出警报。系统还需具备智能监测配电中心环境参数的能力，系统应能实时采集温度、湿度、烟雾浓度等关键环境数据，并将这些信息传输至中央控制系统进行分析处理。这不仅有助于及时发现潜在的安全隐患，还能为维护人员提供必要的参考数据，以便于制定合理的维护计划。

2.2 性能指标

为了确保系统的高效运行，必须设定明确的性能指标。首先，人员识别和区域入侵系统的响应时间需小于 6s。这一要求旨在保证在出现非法入侵时，系统能够在最短时间内做出反应，从而最大限度地减少潜在风险。其次，系统每隔 2min 自动发送一次环境参数监测数据。这种定时数据传输机制不仅提高了数据的实时性和准确性，还便于管理人员及时掌握配电中心的环境状况 [1]。最后，系统设计中必须确保传感器节点通讯的高效性以及从休眠状态激活时延短。

3 系统设计

3.1 数据库设计

3.1.1 数据库架构设计

数据库表主要包括以下几类：

①用户信息表（User_Info）：用于存储系统用户的详细信息，如用户 ID、用户名、密码、权限等级等。该表的设计需考虑数据的安全性和隐私保护，确保敏感信息得到妥善处理。见表 2.1：

【作者简介】翁秋英（1982–），女，中国浙江衢州人，本科，工程师，从事信息技术研究。

表 2.1 用户信息表

列名	说明	数据类型	键码
UserID	唯一标识每个用户	INT	主键
Username	用户的登录名	VARCHAR(50)	
Password	用户的登录密码（加密存储）	VARCHAR(255)	
Role	用户的角色或权限等级	VARCHAR(50)	

②传感器信息表（Sensor_Info）：记录所有传感器的基本信息及其状态，包括传感器 ID、类型、安装位置、当前状态等。见表 2.2：

③环境参数监测数据表（Env_Data）：存储从各传感器采集到的环境参数数据，如温度、湿度、烟雾浓度等，并记录采集时间和传感器 ID。见表 2.3：

④入侵事件记录表（Intrusion_Event）：记录每次人员非正常入侵事件的相关信息，包括事件发生时间、涉及区域、触发原因等。见表 2.4：

表 2.2 传感器信息表

列名	说明	数据类型	键码
SensorID	唯一标识每个传感器	INT	主键
Type	传感器类型（如温度、湿度等）	VARCHAR(50)	
Location	传感器的安装位置	VARCHAR(100)	
Status	传感器当前的工作状态（正常、故障等）	VARCHAR(50)	

表 2.3 环境参数监测数据表

列名	说明	数据类型	键码
DataID	唯一标识每条数据记录	INT	主键
SensorID	对应传感器的信息表中的传感器 ID	INT	外键
Timestamp	数据采集的时间戳	DATETIME	
Temperature	当前温度值	FLOAT	
Humidity	当前湿度值	FLOAT	
SmokeLevel	当前烟雾浓度值	FLOAT	

表 2.4 入侵事件记录表

列名	说明	数据类型	键码
EventID	唯一标识每个入侵事件	INT	主键
Area	发生入侵的区域	VARCHAR(100)	
TriggerTime	事件触发的时间	DATETIME	
Reason	导致入侵的原因描述	TEXT	

3.1.2 数据存储策略和优化措施

为了确保数据库的高效运行，必须采取一系列存储策略和优化措施。在数据存储方面，可以采用分布式数据库技术，将不同类型的表分布存储在多个节点上，以提高查询效率和系统容错能力。针对频繁读写操作的数据表，如环境参数监测数据表，应考虑分区存储，根据时间或其他关键字段进行分区分片，从而减少单个表的数据量，提升查询速度[2]。还需要实施数据压缩技术，并定期进行数据库清理和归档，将过期或不再需要频繁访问的历史数据迁移到冷存储中。在索引设计方面，为常用的查询字段建立合适的索引。通过合理设计索引，可以显著提升查询效率，降低响应时间。最后，为了保障数据安全，必须实施严格的访问控制机制。通过设置不同的权限级别，限制不同角色对数据库的操作权限。还应定期备份数据库，以防数据丢失或损坏。

3.2 系统框架搭建

配电中心智能检测系统的总体架构由硬件和软件两大部分组成。硬件部分主要包括传感器网络、数据采集设备、通信模块以及中央控制系统。传感器网络负责实时监测配电中心的环境参数和人员活动情况，数据采集设备则将这些信息转化为数字信号并进行初步处理。通信模块确保传感器节点与中央控制系统之间的高效数据传输。中央控制系统作为整个系统的“大脑”，负责接收、处理和存储来自各个传感器的数据，并根据预设规则做出相应的决策。

软件部分主要分为四个核心模块：用户管理模块、数据采集与处理模块、数据分析与预警模块以及系统维护与监控模块。用户管理模块负责用户的注册、登录和权限管理，确保不同角色的用户能够访问相应级别的功能。数据采集与处理模块负责从传感器获取原始数据，并对其进行清洗、转换和存储。数据分析与预警模块则利用先进的算法对收集到的数据进行分析，识别异常情况并发出警报。系统维护与监控模块提供系统的健康状态监控、故障诊断及日志记录等功能，确保系统的稳定运行。

3.3 非法入侵算法设计

在入侵检测算法的选择上，采用基于机器学习的分类算法是一种有效的解决方案。具体实现细节包括以下几个步骤：首先，收集大量标注数据作为训练集，这些数据应涵盖正常情况下的各种环境参数和人员活动模式，以及已知的非法入侵事件样本。然后，选择合适的特征提取方法，从原始传感器数据中提取出能够有效区分正常和异常行为的关键特征，如人员轨迹、动作速度、停留时间等。接下来，利用监督学习算法（如支持向量机 SVM、随机森林 RF 或深度神经网络 DNN）进行模型训练，优化模型参数以达到最佳的分类效果。

3.4 环境参数监测算法优化

首先，在数据采集阶段，需要确保传感器能够高精度地采集各类环境参数。这不仅要求选择高质量的传感器硬件，还需要对传感器进行定期校准和维护，以保证数据的准确性。其次，在数据处理阶段，采用滤波算法去除噪声干扰，如卡尔曼滤波或低通滤波器，以提高数据的质量。基于时间序列分析的方法可以用于预测未来一段时间内的环境变化趋势，提前预警可能出现的问题 [3]。

在算法优化方面，可以引入机器学习技术来提升监测系统的智能化水平。利用大数据分析技术，可以从海量的历史数据中挖掘出更多有价值的信息，进一步优化监测策略。还可以结合边缘计算技术，将部分数据分析任务分配给本地设备执行，减少数据传输延迟，提高系统的响应速度。

4 系统测试与验证

4.1 测试方案设计

4.1.1 测试目标

验证系统各模块的功能是否按预期工作；检查系统在不同环境条件下的稳定性和响应速度；确认系统对非法入侵行为的识别准确率和实时性；验证环境参数监测数据的精确性和及时性。

4.1.2 测试环境

硬件配置：数据采集设备：NI CompactDAQ；通信模块：LoRa 模块；中央控制系统服务器：Dell PowerEdge R740，双路 Xeon 处理器、128GB 内存。

软件配置：操作系统：Linux Ubuntu Server 20.04 LTS；数据库 PostgreSQL；应用软件：基于 Python 的自定义应用程序，集成 TensorFlow 和 Scikit-learn 等机器学习库；算法库：OpenCV 用于图像处理，Pandas 和 NumPy 用于数据预处理和分析。

4.1.3 测试用例设计

功能测试：用户管理模块：用户注册、登录、权限设置等功能；数据采集与处理模块：传感器数据的采集、传输、初步处理等；数据分析与预警模块：异常情况识别、警报触发等；系统维护与监控模块：健康状态监控、故障诊断等。

性能测试：响应时间测试：测量从传感器数据采集到系统发出警报的时间间隔；数据传输延迟测试：评估传感器节点与中央控制系统之间的通讯时延；容量测试：验证系统在高负载条件下的稳定性，如同时处理大量传感器数据的能力。

安全性测试：非法入侵检测：模拟不同类型的非法入侵事件，验证系统的识别能力和响应速度；数据加密与访问控制：测试用户认证和权限管理机制的有效性。

环境参数监测测试：精度测试：对比传感器采集的数据与标准值，验证数据的准确性；实时性测试：检查系统每隔 2min 发送一次监测数据的频率和准确性。

4.2 测试结果与分析

4.2.1 功能测试结果

用户管理模块：所有测试用户均能成功注册、登录，并根据权限访问相应功能，无任何错误提示。

数据采集与处理模块：传感器数据能够准确采集并传输至中央控制系统，初步处理后的数据格式正确，无明显噪声干扰。

数据分析与预警模块：系统能够在模拟异常情况下快速识别并发出警报，响应时间均小于 6s。

系统维护与监控模块：系统日志记录完整，健康状态监控和故障诊断功能正常工作。

4.2.2 性能测试结果

响应时间测试：非法入侵检测的平均响应时间为 4.8s，满足设计要求（小于 6s）。

数据传输延迟测试：传感器节点与中央控制系统之间的平均通讯时延为 0.5s，符合高效通讯的要求。

容量测试：系统在同时处理 500 个传感器数据的情况下，仍能保持稳定的响应速度和数据处理能力，未出现卡顿或崩溃现象。

4.2.3 安全性测试结果

非法入侵检测：系统对不同类型非法入侵的识别准确率达到 95% 以上，误报率为 5%，满足实际应用需求。

数据加密与访问控制：未经授权的用户无法访问系统，身份认证和权限控制机制有效。

4.2.4 环境参数监测测试结果

精度测试：传感器采集的温度、湿度、烟雾浓度等数据与标准值的误差均在 ±2% 以内，符合设计要求。

实时性测试：系统每隔 2min 准时发送一次监测数据，数据完整且准确，未发现丢失或延迟现象。

5 结语

本研究旨在开发一款基于物联网技术的配电中心智能检测系统，以提高配电中心的安全性和管理效率。经过全面的测试和验证，系统在功能完备性、性能优越性、安全性和环境参数监测精准性等方面均表现出色，能够满足应用需求。

参考文献

[1] 崔琰,孙一轩.基于视频AI识别的智能变电站检测系统设计与实现[J].家电维修,2024,(11):110-112.

[2] 丁思远.防触电消防安全指示灯设计及智能检测系统[J].灯与照明,2023,47(02):39-42.

[3] 郭瑶.针对智能合约的安全检测系统设计与实现[D].北京邮电大学,2023.