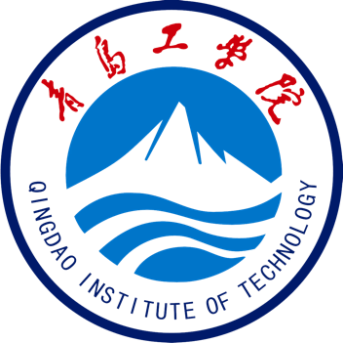


本科毕业论文（设计）开题报告



|  |  |
| --- | --- |
| 题目 | 《面向智慧校园物联网设备的IDS安全  防护方案优化与实现》 |
| 学院 | 人工智能与大数据学院 |
| 年级专业 | 2022级信息安全专业 |
| 学生姓名 | 刘逸菲 |
| 学号 | 2021121150111 |
| 指导教师 | 孙德森 |

教务处制表

|  |
| --- |
| **一、选题依据**（选题来源与背景，研究目的，国内外研究现状，主要参考文献） |
| 1. （一）**选题来源与背景**   **1.选题来源:**源于智慧校园物联网化进程中，设备激增导致的传统入侵检测系统(IDS)“误报率高、适配性差、响应滞后”等实际痛点，属于工程实践驱动型选题。  **2.选题背景:**智慧校园已接入门禁、监控、环境监测等数千台物联网设备，这类设备普遍存在“算力低、无加密、协议多样”的特性，成为网络攻击突破口(如2024年某高校物联网摄像头被植入恶意代码导致隐私泄露)。而传统IDS多针对 PC端设计，无法适配物联网设备的轻量化需求，防护效果大幅下降，需针对性优化  （二）**研究目的**  1.解决传统IDS在智慧校园物联网场景下的三大核心问题:降低对低算力设备的资源占用率、减少因协议不兼容导致的误报、提升对物联网特有的“异常数据采集”“设备仿冒”等攻击的检测精度。  2.设计并实现一套轻量化、高适配的IDS优化方案，最终通过实验验证方案在智慧校园物联网环境中的有效性，为校园网络安全防护提供可落地的技术参考。  （三）**国内外研究现状**  **1.国外研究现状**  (MIT)团队提出基于联邦学习的物联网 IDS，在保护设备数据隐私的同时提升检测模型精度，已在部分高校试点，但存在部署成本高的问题。 标准与实践结合:美国国家标准与技术研究院(NIST)发布《物联网设备安全指南》，明确IDS需支持LoRa、ZigBee等校园常用物联网协议，思科、Palo Alto等企业已推出适配性较强的商业IDS，但对校园场景的定制化不足。  国外在物联网IDS领域起步较早:Neto等人(2023)发布CICloT2023数据集，为物联网大规模攻击检测提供了基准测试平台;Altan(2021)提出SecureDeepNet- loT深度学习入侵检测模型，适用于工业物联网场景，检测准确率达93%，但资源消耗较高;Heartfield等人(2021)基于强化学习实现智能家居自配置入侵检测，泛化能力强，但未适配校园多设备协同场景。国外研究在算法精度和数据集建设上有优势，但针对智慧校园的定制化优化不足，且商业方案成本较高，难以在高校大规模推广。  **2.国内研究现状**  侧重“轻量化与场景适配”:清华大学网络安全实验室针对智慧校园，提出“特征提取+边缘计算”的IDS优化思路，将部分检测任务下沉到边缘网关，降低设备算力压力，但模型对新型攻击的泛化能力较弱。  政策驱动研究:教育部在《教育信息化2.0行动计划》中要求高校加强物联网设备安全防护，国内企业(如奇安信、深信服)推出校园专用IDS产品，但核心检测算法多基于传统规则，对“零日攻击”的识别能力不足.  国内学者围绕校园物联网安全展开了相关研究:杨阳(2025)提出融合CNN深度学习算法的校园网络入侵检测方案，检测准确率达89%，但模型复杂度高，难以适配低算力设备;《高校网络安全技术防护方案设计》(2025)构建了分层防护体系，但未针对物联网设备的特殊性优化IDS核心算法;《2025年物联网设备安全漏洞分析与防护技术在智慧教育中的应用报告》指出了固件加固、协议安全等防护方向，但缺乏具体的检测系统实现方案。总体来看，国内研究多侧重理论架构或单一技术应用，尚未形成“算法轻量化+场景定制化+系统可落地”的完整解决方案。  **（四）主要参考文献**  **1.国内：**  （1）王健.智慧校园物联网设备安全防护技术研究[J].计算机工程,2023,49(5):  （2）刘芳,张伟.边缘计算与物联网融合的安全防护技术研究[J].通信学报,2022，43(8):156-168.  （3）(美)克里斯·桑德斯,(美)保罗·普罗沃斯.入侵检测原理与实践[M].北京:机械工业出版社,2021.  （4）张建国,陈静.智慧校园物联网安全风险分析与防护策略[J].中国教育网络，2023(2):4、5-48.  （5）杨阳.智慧校园的网络安全防护体系构建与研究[J].网络空间安全，2025，14(5):81-84.  （6）张明,李军.高校网络安全防护解决方案[J].计算机工程与应用，2025，61(3):123-129.  （7）陈晨,赵伟.基于改进随机森林的物联网入侵检测算法研究[J].计算机应用研究，2024,41(7):2089-2093.  （8）李娜,张华.边缘计算在校园物联网安全中的应用研究[J].现代电子技术，2024，47(12):135-139.  （9）刘伟,陈明.智慧校园物联网多协议适配安全机制设计[J].通信技术，2023，56(8):1890-1896.  **2.国外：**  （1）Neto, E.C. P., et al.CICloT2023: AReal-Time Dataset for IoT Attacks[J]. Sensors,2023.  （2）Khan, A. S., et al. Lightweight IDS forIoT Devices in Smart Campuses[J]. Journal of Network and Computer Applications,2024. |

|  |
| --- |
| **二、研究内容**（研究内容，研究思路，研究方法） |
| **（一）研究内容**  首先分析智慧校园物联网设备特征与安全风险，包括门禁、传感器、监控摄像头等设备的算力、协议、数据传输等特点，识别设备接入、数据传输、设备自身环节的安全风险防护，明确传统IDS在该场景的不足。  从数据采集处理机制、系统架构两方面优化IDS安全防护方案：  1. 改进数据采集与处理机制：针对校园物联网多源数据格式不统一的问题，在边缘终端增加轻量化数据预处理模块——按安全编码规范过滤无效、恶意数据，再对不同设备的原始数据精简既降低数据传输负载，也提升后续检测的效率。  1.优化系统架构：设计“边缘终端本地预处理-校园服务器集中检测”的分层架构，让边缘设备仅负责数据初步清洗，核心检测任务由服务器承担，兼顾轻量设备的算力限制与检测的准确性。  2.最终搭建模拟测试环境，还原校园物联网模拟端口扫描、非法登录等攻击场面，通过检测准确率、误报率、资源占用率、响应时间等情况验证方案的有效性，为智慧校园物联网安全防护提供技术支持。  **（二）研究思路**  按照“调研分析→方案优化→测试验证→总结应用”的步骤推进：  1. 现状与风险调研：先调研校园物联网中门禁、传感器、监控摄像头等设备的实际部署情况，分析其算力、协议、数据传输等特征，梳理设备接入、数据传输、终端自身的安全风险，明确传统IDS在该场景下的适配不足；  2. 方案设计：针对上述不足，从两个维度优化IDS安全防护方案——一是改进数据采集与处理机制，在边缘终端增设轻量化预处理模块；二是优化系统架构，搭建“边缘预处理-服务器集中检测”的分层模式；  3. 模拟环境测试：搭建还原校园物联网的测试环境，模拟端口扫描、非法登录等典型攻击场景，通过检测准确率、误报率等指标验证优化方案的有效性；  4. 总结与应用：总结方案的适配效果，明确其对智慧校园物联网安全防护的技术支持，同时梳理后续可拓展的研究方向。  **（三）研究方法**  1. 基于入侵检测基础理论选技术：参考《入侵检测技术》课程里的特征匹配、异常检测知识，用“简单特征匹配”结合的方式——特征匹配靠已知攻击特征码识别常见攻击，异常检测靠学习设备正常行为找异常，既贴合专业知识，又不用复杂操作。  2. 按安全编码规范写代码：遵循课程里讲的基础安全编码要求，比如过滤无效数据、不用有漏洞的开源库版本，用Python写核心模块（数据采集、检测功能），确保代码本身安全，同时方便调试修改。  3. 按网络安全实验思路搭测试环境：跟着《网络安全实验》里的模拟实验方法，用45台虚拟设备+5台实体设备搭校园物联网环境，还原简单的设备连接拓扑；再模拟端口扫描、非法登录这些常见攻击场景，生成10000+条测试数据，不用搞复杂攻击。  4. 用基础安全指标做测试验证：参考专业里的简单性能评估标准，重点测4个核心指标——检测准确率、误报率、设备资源占用率、响应时间，做200+次测试，记录数据后对比优化效果，不用深入分析复杂指标。  5. 结合物联网安全基础做数据处理：依据《物联网安全》里的协议解析知识，通过常用协议的数据分析，提取关键信息；同时用基础的AES加密方法保护测试数据，避免传输时被篡改，符合信息安全的基本要求。 |

1. **进度安排**

|  |  |
| --- | --- |
| **起止时间** | **主要内容** |
| 2025.11.04—2026.01.08 | 课题选择，确定论文题目，查阅文献，准备开题报告，完成开题答辩 |
| 2026.01.09—2026.02.25 | 完成方案总体设计及详细设计，编写方案文档并进行设计验证 |
| 2026.02.26—2026.03.16 | 完成方案各部分的测试与验证工作，确保方案功能和性能符合预期 |
| 2026.03.17—2026.05.11 | 撰写论文，完成论文初稿，并根据指导老师反馈修订，完成论文终稿 |
| 2026.05.12—2026.06.10 | 完成毕业答辩，修改论文并根据答辩意见修订，完成论文归档 |

|  |  |  |
| --- | --- | --- |
| **四、审核意见** | | |
| 指导教师意见： | | |
| 指导教师签名: | | 年月日 |
| 开题评议结果 | | 开题小组组长签名 |
| 合格【】 | 不合格【】 | 年月日 |

注：表格预留高度和行数如果不够可自行调整。