大学生论文检测系统

文本复制检测报告单(全文标明引文)

№:ADBD2023R_20230530193355472635798340　　检测时间:2023-05-30 19:33:55

篇名: 工控网络攻击路径模拟与分析系统设计与实现

作者: 孙畅

指导教师: 宋轩

检测机构: 南方科技大学

文件名: 11910437_孙畅_毕设论文_中文.pdf

检测系统: 大学生论文检测系统

检测类型: 大学生论文

检测范围: 中国学术期刊网络出版总库
中国博士学位论文全文数据库/中国优秀硕士学位论文全文数据库
中国重要会议论文全文数据库
中国重要报纸全文数据库
中国专利全文数据库
图书资源
优先出版文献库
大学生论文联合比对库
互联网资源(包含贴吧等论坛资源)
英文数据库(涵盖期刊、博硕、会议的英文数据以及德国Springer、英国Taylor&Francis 期刊数据库等)
港澳台学术文献库
互联网文档资源
源代码库
CNKI大成编客-原创作品库
机构自建比对库

时间范围: 1900-01-01至2023-05-30

检测结果

去除本人文献复制比: 4%　　跨语言检测结果: -

去除引用文献复制比: 2.2%　　总文字复制比: 4%

单篇最大文字复制比: 1.7% (攻击图技术应用研究综述 - 道客巴巴)

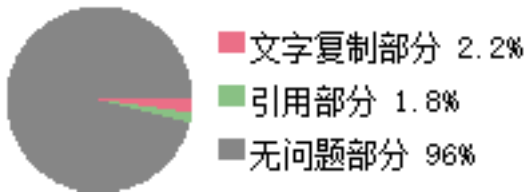
重复字数: [682]　　总段落数: [2]

总字数: [17219]　　疑似段落数: [2]

单篇最大重复字数: [297]　　前部重合字数: [5]

疑似段落最大重合字数: [593]　　后部重合字数: [677]

疑似段落最小重合字数: [89]



指标: ☐ 疑似剽窃观点　☑ 疑似剽窃文字表述　☐ 疑似整体剽窃　☐ 过度引用

相似表格: 0　　相似公式: 没有公式　　疑似文字的图片: 0

5.5%(593)	5.5%(593)	工控网络攻击路径模拟与分析系统设计与实现_第1部分（总10808字）
1.4%(89)	1.4%(89)	工控网络攻击路径模拟与分析系统设计与实现_第2部分（总6411字）

（注释: 无问题部分　文字复制部分　引用部分）

指导教师审查结果

指导教师：　宋轩

审阅结果：

审阅意见：　指导老师未填写审阅意见

1. 工控网络攻击路径模拟与分析系统设计与实现_第1部分　总字数：10808

相似文献列表

去除本人文献复制比：5.5%(593)　文字复制比：5.5%(593)　疑似剽窃观点：(0)

1	攻击图技术应用研究综述 - 道客巴巴 - 《互联网文档资源（https://www.doc88.co）》- 2020	2.7%（297） 是否引证：否
2	攻击图技术应用研究综述 叶子维;郭渊博;王宸东;琚安康; - 《通信学报》- 2017-11-25	2.7%（291） 是否引证：是
3	基于活动社交网络的推荐系统设计与实现 李游(导师：余文) - 《北京邮电大学硕士论文》- 2021-05-31	0.6%（66） 是否引证：否
4	黄兆芳_1120420210_个人理财系统的设计与开发 黄兆芳 - 《大学生论文联合比对库》- 2015-04-29	0.6%（60） 是否引证：否
5	黄兆芳_1120420210_个人理财系统的设计与开发 黄兆芳 - 《大学生论文联合比对库》- 2015-04-30	0.6%（60） 是否引证：否
6	SOPC分析仪器信息管理及系统调试 唐咏;刘书凯; - 《物联网技术》- 2013-10-15	0.3%（37） 是否引证：否
7	人力资源管理系统的设计与实现 张恩宽(导师：罗光春;谭树成) - 《电子科技大学硕士论文》- 2012-03-01	0.3%（37） 是否引证：否
8	基于JakartaEE的招聘网站设计与实现 叶晨 - 《大学生论文联合比对库》- 2019-05-04	0.3%（33） 是否引证：否
9	商品义卖网站设计与实现 马艳红;邢秀婷; - 《电脑编程技巧与维护》- 2011-11-03	0.3%（33） 是否引证：否
10	5525682_梁欣燕_面向网络爬虫的教学舆情分析系统的设计与实现 梁欣燕 - 《大学生论文联合比对库》- 2018-06-09	0.3%（30） 是否引证：否
11	居民用水量分析预测系统设计与实现 张骞(导师：付必涛) - 《华中科技大学硕士论文》- 2021-05-20	0.3%（29） 是否引证：否

原文内容

分类号编号
U D C 密级
本科生毕业设计（论文）
题目：　工控网络攻击路径模拟与分析系统设计与实现
姓名：　孙畅
学号：　11910437
系别：　计算机科学与工程系
专业：　计算机科学与技术
指导教师：　宋轩副教授
2023 年 6 月 2 日
诚信承诺书
1. 本人郑重承诺所呈交的毕业设计（论文），是在导师的指导下，
独立进行研究工作所取得的成果，所有数据、图片资料均真实可靠。
2. 除文中已经注明引用的内容外，本论文不包含任何其他人或
集体已经发表或撰写过的作品或成果。对本论文的研究作出重要贡献的个人和集体，均已在文中以明确的方式标明。
3. 本人承诺在毕业论文（设计）选题和研究内容过程中没有抄袭
他人研究成果和伪造相关数据等行为。
4. 在毕业论文（设计）中对侵犯任何方面知识产权的行为，由本

人承担相应的法律责任。
作者签名:
年月日工控网络攻击路径模拟与分析系统设计与实现孙畅
（计算机科学与工程系指导教师：宋轩）
[摘要]：随着科技的不断发展和进步，越来越多的工业控制系统开始采
用计算机网络和技术。这些技术的应用在提高生产力的同时也带来了一
些安全隐患，网络安全研究成为当前备受关注的热点课题。基于攻击图的安全建模和分析技术可用于实现网络攻击路径模拟和安全分析，通过建立工控网络安全模型、描述各个节点之间的关系及漏洞情况，可以预测并模拟攻击者可能采取的攻击路径和攻击方式，帮助企业及时采取相应的安全措施保护网络安全。工控网络中的警报数据是评估系统安全性、
进行故障维护和优化系统性能的重要指标之一。本文设计并实现了一个基于警报数据的工控网络攻击路径模拟与分析系统，该系统采用 B/S 架构，根据报警管理关联规则实现了攻击路径的可视化展示与管理，预测攻击者可能采取的攻击路径和手段，为防范和应对网络攻击提供了理论支持。该研究课题具有前瞻性和实用性，在工控系统网络安全领域具有很大应用前景。
[关键词]：工控网络，攻击图生成，警报数据，安全建模
I
[ABSTRACT]: With the continuous development and progress of technology, more and more industrial control systems are adopting computer networks and technologies. The application of these technologies not only improves productivity, but also brings some security risks. In recent years, multiple network attacks targeting industrial control systems have occurred frequently. Network security research has become a hot topic of concern. Security modeling and analysis technology based on attack graphs can be used to simulate network attack paths and do security analysis. By establishing a security model of industrial control networks, the relationships and vulnerabilities between nodes can be described. Accordingly, possible attack paths and methods that attackers may adopt can be predicted and simulated. Therefore, a good security model for industrial control networks can help enterprises take corresponding security measures in a timely manner. Alarm data in industrial control systems networks is one of the important indicators for evaluating system security, performing fault maintenance, and optimizing system performance. The paper designs and implements an industrial control systems network attack path simulation and analysis system based on alert data. The system adopts a B/S architecture, and realizes the visual display and management of attack paths based on alarm management association rules. By analyzing the attack graph, possible attack paths and methods that attackers may adopt can be predicted effectively. This provides theoretical support for preventing and responding to network attacks. This research topic has forward-looking and practical significance, and has great application prospects in the field of network security for industrial control systems.
[Key words]: Industrial Control Systems Network, Attack Graph Generation, Alert Data, Security Modeling
II
目录

1. 绪论

1.1 背景及研究的目的和意义

工业控制系统（Industrial Control System，ICS）作为现代生产中的重要组成部分，在推动经济发展和提高生产效率等方面扮演着不可替代的角色。互联网的快速发展使其在 ICS 中的应用逐渐增多，由于 ICS 的特殊性，ICS 更加容易受到专门攻击软件和攻击工具的攻击[1]，并且 ICS 漏洞可能会对企业生产安全造成严重影响，甚至引发国家安全危机。近年来，多起针对 ICS 的网络攻击事件频繁发生，例如 Stuxnet 病毒攻击事件[2]、乌克兰电网攻击事件[3]和 WannaCry 勒索病毒攻击事件[4]等，这些事件严重破坏了工业基础设施的正常运营，直接影响了国家和人民的经济利益与安全。然而，工业控制系统的发展目前还远不成熟，对于 ICS 网络安全的研究十分迫切，同时这也是当前备受关注的热点课题[5]。

攻击图是一种用于描述系统安全缺陷的图形化工具，已广泛应用于工控网络安全研究，也是评估和设计工业控制系统（ICS）安全的重要工具[6-7]。通过攻击图，研究人员可以识别系统中的漏洞和威胁，并预测恶意攻击者可能采取的攻击路径。这些信息可以指导研究人员开发出更好的防御机制，以更好地保护工控系统安全[8-11]。

工控网络中的警报数据是评估系统安全性、进行故障维护和优化系统性能的重要指标之一。通过对警报数据的分析，可以快速发现网络中的异常流量和威胁行为，并识别网络攻击的类型，有助于实现准确的攻击检测和快速响应。此外，警报数据还可以用于预测设备的故障和损坏，提高生产效率和维护效益。

本研究旨在设计并实现一个基于警报数据的工控网络攻击路径模拟与分析系统，以典型的工业控制系统为例，捕获并分析警报数据，研究系统的物理层和网络层易受到攻击的脆弱点，深入了解系统可能面临的攻击方式，如拒绝服务攻击、数据注入攻击、数据窃取攻击等[12]，为系统生成攻击路径，分析多步攻击模式，构建攻击场景。

本系统为基于 WEB 的攻击路径生成与管理系统，实现警报数据的展示与分析，动态生成攻击路径的图像化展示，识别关键脆弱点。基于 WEB 的攻击图生成技术可以帮助分析人员更直观地了解系统的安全风险、脆弱点和漏洞，为安全评估、漏洞挖掘、

安全决策等提供重要依据和支持[11,13-14]。本研究课题具有前瞻性和实用性，为信息安 1

全防护设计提供理论支撑，在工控系统网络安全领域具有很大应用前景。

1.2 相关工作

攻击图的研究始于 20 世纪 90 年代，Philips 和 Swiler 首次提出了攻击图的概念，并将其应用于网络脆弱性分析[15]。目前，已有多种攻击图生成和分析工具，如MulVAL、NetSPA、TVA 等。MulVAL 是由 Ou 等[16]开发的 Linux 平台开源攻击图生成工具，使用 graphviz 图片生成器绘制攻击图，输出文件为 pdf 或 txt 格式，具有较好的准确度和可拓展性。NetSPA 是由 Lippmann[17]提出的一种基于图论的生成工具，

使用防火墙规则和漏洞扫描结果构建网络模型，规则库需要手动输入。TVA 是一款可用于对网络渗透进行自动化分析的攻击图生成工具，输出结果为由攻击步骤和攻击条件构成的状态攻击图，Cauldron 是 TVA 的商用版[18]。

目前，攻击图已广泛应用于工业控制网络方面的研究。徐丽娟[19]根据工控网络的特点，提出了一种适用于工控系统的攻击图分层生成算法，在工控网络的分析中比MulVAL 有更好的效率。黄家辉等[20]对 ICS 中的工艺流程的多项指标进行评估，制定了一套 ICS 漏洞等级划分标准，基于攻击图对 ICS 脆弱性进行量化评估。

攻击图也广泛应用于入侵检测和报警关联方面，如风险评估与网络加固等。Ahmad 等[21]通过将攻击图生成工具 MulVAL 和入侵检测系统 SNORT 结合，从概念上证明了将攻击图工具与入侵检测系统结合，可以实现攻击过程中的实时防御。Seyed

等[22]提出了一种基于攻击图的混合报警关联模型，但未能对后续攻击进行准确的预测。刘威歆等[23]提出了一种基于攻击图的多源报警关联分析方法，具有较好的准确性，并行化的设计使其具有较快的分析速度[18]。

1.3 主要研究内容和结构安排

本研究旨在设计并实现一个基于警报数据的工控网络攻击路径模拟与分析系统，系统采用 B/S 架构，实现警报数据的管理、分析与展示，基于警报数据生成攻击图数

据，动态生成并展示攻击路径，同时展示对攻击图数据的分析结果。系统的主要功能模块包括注册与登录、系统主页展示、警报信息展示、攻击路径的生成与查看、数据管理和系统管理等，详细介绍见 2.1 功能性需求分析与 3.1 功能模块划分。

论文在结构上共分为 7 章，具体内容如下所示。 2

1. 绪论：介绍本课题的研究背景与研究意义、相关工作和课题的主要研究内容。
2. 系统需求分析：采用用例图描述系统功能，并介绍系统开发环境和开发工具。
3. 系统概要设计：介绍系统的功能模块划分、架构设计与总体部署。
4. 系统详细设计：对本课题使用的数据进行说明，并详细介绍了系统的数据库设

计与接口设计。
5. 系统实现：展示系统功能。
6. 系统测试：对系统的功能和性能进行测试。
7. 总结：对研究进行总结。
2. 系统需求分析
2.1 功能性需求分析
本系统有两种权限角色：普通用户与管理员。管理员和普通用户在大多数功能上具有相同的操作权限，包括登录、查看系统主页、警报数据的统计与管理、攻击图的生成与查看、资源统计和用户管理等。然而，用户管理模块是管理员与普通用户区分开来的关键。管理员具有对所有用户的管理权限，包括查看用户信息，添加、修改、删除用户等操作；而普通用户则只能对自己账户密码进行修改。此外，新注册的用户均为普通用户，除非管理员设置其为管理员。为了更好地呈现权限差别，描述系统功能，本文根据不同用户角色绘制了对应的用例图如下。
图2-1-1为管理员用户的用例图，展示了管理员用户的基本功能需求。 3
图 2-1-1 管理员用户用例图图5-6-2为普通用户的用例图，展示了普通用户的基本功能需求。
图 2-1-2 普通用户用例图
2.2 系统开发环境与开发工具
为使系统具有较好的可移植性，本系统部署在 Ubuntu Linux 操作系统的虚拟机上，使用 docker 部署数据库，其硬件开发环境和软件开发环境分别如表2-2-1和表2-
2-2所示。 4
表 2-2-1 系统硬件开发环境表
硬件环境规格说明
设备名称 LAPTOP-25S1TULK
处理器 Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
机带 RAM 8.00GB
操作系统 Windows 64 位操作系统，基于 x64 的处理器表 2-2-2 系统软件开发环境表
软件环境规格说明
操作系统 Ubuntu Linux 64-Bit
Docker v20.10.21
本系统采用 B/S 架构，前端使用 Vue 框架开发，使用了 D3.js, Echarts, Element,Axios, Vuex 等技术组件，后端使用 Flask 框架开发，使用 PyMongo 进行数据库的连接，使用 NetworkX 进行图数据的处理，数据库使用 MongoDB，使用 MongoDB Compass
进行数据库表的管理。系统开发语言及工具表如表2-2-3所示。
表 2-2-3 系统开发语言及工具表列名工具名与版本号系统开发语言 HTML, JavaScript, CSS(前端), Python(后端)
系统开发框架 Vue2.9.6(前端), Flask(后端)
前端技术组件 Echarts, Element, Vuex, Axios, D3.js
后端技术组件 PyMongo, NetworkX
系统开发工具 WebStorm2021.1.2 x64, PyCharm2021.2.3
数据库操作工具 MongoDB Compass
数据库 MongoDB v5.0.5
3. 系统概要设计
3.1 功能模块划分
本系统为基于工控网络中警报数据的攻击路径模拟与分析系统，其功能模块划分如图3-1-1所示。 5
1. 注册与登录：实现用户的注册与登录。
• 登录：用户输入用户名、密码，点击登录，登录成功进入系统主页。
• 注册：用户输入用户名、密码并确认密码，点击注册，注册成功后自动登录跳转至系统主页。新注册的用户均为普通用户。
2. 系统主页：实现警报数据表、词云图与威胁评分折线图的展示。
3. 警报数据展示：展示警报数据的统计图表，包括攻击类型的数量随时间变化折
线图、警报数量随时间变化折线图、攻击类型与攻击名称树状图和不同等级的警报数量扇形图。
4. 攻击路径管理：分为两个页面，实现传感器层攻击图与网络层攻击图的展示，侧
边栏展示攻击图信息与所选节点信息的统计数据。
5. 数据管理：对警报数据进行查看与管理，用户可以根据查询条件筛选数据进行
查看。
6. 系统管理：分为资源统计与用户管理两个页面。
• 资源统计：页面左侧展示用户登录登出日志信息表，右侧从上到下展示系统时间与资源利用率，包括 CPU、内存、硬盘的利用率。
• 用户管理：根据不同用户权限进行展示，管理员可以查看用户信息表，添加、修改或删除用户，普通用户可以修改密码。 6
图 3-1-1 攻击路径模拟与分析系统功能模块图
3.2 系统架构设计
系统采用 B/S 架构，主要分为表现层、服务层与数据层，如图3-2-1所示。
表现层又称 UI 层，展示系统网页界面，包含登录/注册、系统主页、警报展示、

攻击路径展示、数据管理、资源统计与用户管理页面等。该层采用 Vue 框架，作为网页的主体，使用 Element UI 等组件设计页面，使用 D3.js 和 Echarts 等组件展示数据。该层采用 HTTP 请求进行前后端的连接，使用 Axios 组件发送请求。前端通过调用 api 接口，向服务端发送请求。这些请求可以是各种类型的操作，如获取数据、更新数据、删除数据等。

服务层分为控制层和业务逻辑层，用于处理前端请求和数据库管理。使用 Python 7

的 Flask 框架，Flask-app 用于接收和响应 HTTP 请求，服务层和数据层使用 PyMongo进行交互，对数据库进行增、删、改、查的操作。

数据层由数据访问层和数据存储层构成，数据访问层用于进行后端与数据库的交互，数据存储层用于数据存储，使用 MongoDB 存储数据。

图 3-2-1 系统架构图

3.3 系统总体部署

本系统采用了 B/S 架构，服务端部署在基于 Linux 操作系统的虚拟机中，数据库服务器使用 MongoDB。运维人员只需要对服务端进行维护管理，无需关注客户端的部署细节。用户可以通过浏览器访问系统界面，与服务端进行交互。

数据库服务器与服务端之间通过 TCP 连接进行通信，以保证数据的稳定和可靠性。同时，系统前端使用网页浏览器作为客户端，通过 HTTP 协议进行与服务端的通信，具有较好的兼容性和易用性。

系统的前端部分使用 npm 进行打包，后端使用 app.py 启动框架。该设计使本系统具有较好的可扩展性和可维护性。系统部署图如图3-3-1所示。 8

图 3-3-1 系统部署图

4. 系统详细设计

4.1 数据说明

本课题的原始数据集来源于 4SICS Geek Lounge 的抓包文件1。4SICS（现称为

CS3Sthlm），即斯德哥尔摩监控与数据采集系统（Supervisory Control and Data Acqui-

sition, SCADA）和工业控制系统（ICS）网络安全国际峰会，其中的 Geek Lounge 包含一个 ICS 实验室，本课题使用的数据集为 Netresec 捕获的该 ICS 实验室的网络流量包。

Snort 是目前全球最著名的开源入侵防范系统（Intrusion Prevention System, IPS）。

Snort IPS 使用一系列规则来定义恶意网络活动，通过这些规则来查找与之匹配的数据包并为用户生成警报。Lenny Hansson 基于上述 PCAP 文件（即网络流量包）创建了 Snort 规则，可用于资产检测与提供安全警报。本课题使用 Snort 软件对原始 PCAP

文件进行处理，根据 Lenny 的 Snort 规则进行解析，生成警报数据。经处理后的警报数据包含 9 个字段，警报 Id、攻击名称、攻击类型、警报等级、时间、源 IP 与源端

口号、目的 IP 与目的端口号。基于警报数据生成网络层攻击图数据、词云图数据与

警报的威胁评分数据。

4.2 数据库设计

本系统使用 Mongo 数据库存储数据信息，数据库部署在 Linux 系统的虚拟机上，数据库表介绍如表4-2-1所示。

1数据来源：https://www.netresec.com/?page=PCAP4SICS 9

表 4-2-1 数据库表介绍表

表中文名称表英文名称说明

用户表 user 存储用户基本信息用户日志表 userlog 存储用户登录登出信息警报数据表 alarm 存储警报数据信息攻击类型与攻击名称表 alarmClassify 存储攻击类型与对应的攻击名称计数表 counters 存储不同类型数据的数量威胁评分表 resScore 存储不同时间下威胁评分信息传感器层攻击图数据表 PhysicsGraph 存储传感器层攻击图数据网络层攻击图数据表 NetGraph 存储网络层攻击图数据网络层攻击图展开图数据表 NetGraphAll 存储网络层攻击图展开图数据网络层两节点间的攻击路径表 NetPathGraph 存储网络层两节点间的攻击路径数据

系统数据库具体表的设计说明如下。

用户表 user 存储了在本系统已注册的用户信息。其中 username 为不重复字段，为登录的用户名。用户表 user 设计如表4-2-2所示。

表 4-2-2 用户表列名数据类型字段描述

_id ObjectId 主键，对象 Id

userId Int32 用户 Id

userName String 不重复字段，用户名

role String 用户权限

regTime String 用户的注册时间

password String 用户密码用户日志表 userlog 存储了用户的登录登出信息，包括用户名、用户 ip 地址、登录登出时间、登录 Id，其设计如表4-2-3所示。 10

表 4-2-3 用户日志表列名数据类型字段描述

_id ObjectId 主键，对象 Id

LogoutTime String 用户的登出时间

LoginTime String 用户的登录时间

name String 用户名

ip String 用户登录的 ip 地址

loginId String 登录 Id

警报数据表 alarm 存储了警报数据信息，包括警报 Id、攻击名称和攻击类型、警

报等级、时间、源 IP 和源端口号、目的 IP 和目的端口号等信息，其设计如表4-2-4所

示。
表 4-2-4 警报数据表列名数据类型字段描述
_id ObjectId 主键，对象 Id
al_id Int32 警报 Id
atk_name String 攻击名称
classification String 攻击类型
level String 警报等级
time String 时间
sip String 源 IP
sport String 源端口号
dip String 目的 IP
dport String 目的端口号
format_time1 String “yyyy-MM-dd HH:mm:ss”格式的时间
format_time2 String 微秒 (小数点后 6 位)
攻击类型与攻击名称表 alarmClassify 存储了攻击类型与攻击名称的对应关系，即每个攻击名称对应的攻击类型，其设计如表4-2-5所示。 11
表 4-2-5 攻击类型与攻击名称表列名数据类型字段描述
_id ObjectId 主键，对象 Id
classification String 攻击类型
atk_name String 攻击名称计数表 counter 存储了不同类型数据的数量，其设计如表4-2-6所示。
表 4-2-6 计数表列名数据类型字段描述
_id String 不重复字段，数据类型名称
id String 该类型数据数量，也是最后一条数据的 Id
威胁评分表 resScore 存储了不同时间下的威胁评分信息，包括时间、通信主机 ip和威胁评分，其设计如表4-2-7所示。
表 4-2-7 威胁评分表列名数据类型字段描述
_id ObjectId 主键，对象 Id
ip String 通信主机 ip
score String 威胁评分
time String 时间传感器层攻击图数据表 PhysicsGraph 存储传感器层攻击图的数据，包括节点集和边集，其设计如表4-2-8所示。
表 4-2-8 传感器层攻击图数据表列名数据类型字段描述
_id ObjectId 主键，对象 Id
nodes Array 攻击图节点数据集
edges Array 攻击图边数据集 12
传感器层节点数据描述如表4-2-9所示。边数据由源节点 Id(source) 和目的节点
Id(target) 构成。
表 4-2-9 传感器层节点数据描述表
字段名数据类型字段描述
id Int32 不重复字段，节点 Id
sensor String 传感器名称
alarm String 报警中文名称
name String 报警英文名称
image String 节点对应的图片地址网络层攻击图数据表 NetGraph 存储了网络层攻击图的数据，网络层攻击图展开图数据表 NetGraphAll 存储了其展开图的数据，二者包含的字段相同，包括设备集、
节点集、设备边集和总边集，其设计如表4-2-10所示。
表 4-2-10 网络层攻击图数据表列名数据类型字段描述
_id ObjectId 主键，对象 Id
devices Array 设备节点数据集
nodes Array 总节点数据集，包括设备节点和攻击节点
edgesDev Array 设备边集
edges Array 总边集，包含攻击图的全部边网络层节点分为设备节点 device 和攻击节点 vulnerability，二者节点名称不同，设备节点为设备 IP，攻击节点为攻击名称。此外，设备类型 device 和图片地址 image 为设备节点的独有字段。网络层节点数据描述如表4-2-11所示。
与传感器层相同，网络层的边同样由源节点 Id (source) 和目的节点 Id (target) 构
成。 13
表 4-2-11 传感器层节点数据描述表
字段名数据类型字段描述
id Int32 不重复字段，节点 Id
name String 节点名称，设备节点为设备 IP，攻击节点为攻击名称
type String 节点类型
device String 设备节点独有，设备类型

image String 设备节点独有，节点对应的图片地址网络层两节点间的攻击路径表 NetPathGraph 存储了网络层攻击图两节点间的攻

击路径，两节点为源节点（source）和目的节点（target），其设计如表4-2-12所示。

该数据表的作用是提高按深度搜索网络层攻击图数据的效率。由于网络层攻击图攻击节点数量庞大，注意到攻击节点仅存在于两个设备节点之间，本文采取存储两个设备节点之间的攻击路径的方式存储攻击节点信息，单独存储设备节点与设备节点之间的对应边，这样的方式成功的缩小了攻击图的体量，也提升了数据搜索的速度。

表 4-2-12 网络层两节点间的攻击路径表列名数据类型字段描述

_id ObjectId 主键，对象 Id

source String 源节点设备 IP

target String 目的节点设备 IP

depth Int32 攻击路径深度

graph Object 该路径对应的攻击图网络层两节点间的攻击路径表中的 graph 字段为该路径对应的攻击图数据，为包含节点集（nodes）和边集（edges）的字典，节点集和边集的数据类型均为 Array，包含的节点的字段与网络层攻击图数据表的 nodes 和 edges 相同，其中设备节点的 Id 与网络层攻击图数据表中的设备节点 Id 相对应。

4.3 接口设计

本系统采用 B/S 架构，前端页面通过 HTTP 请求向后端服务器发送请求，后端服务器使用 Flask 框架进行处理并响应客户端的请求。Flask 框架在接收到客户端请求 14

后，会根据请求的参数（如请求方法、URL 等）在接口表中查找相应的接口，并将请求转发给对应的后台逻辑处理模块进行处理。后台逻辑处理模块处理完毕后，将结

果返回给 Flask 应用程序，Flask 应用程序再将结果打包成 HTTP 响应返回给客户端。

通过这种方式，实现了前后端数据的交互和协议、端口和地址的统一管理，提高了开发效率和代码可维护性。本系统接口设计如表4-3-1所示。

表 4-3-1 接口设计表

接口 URL 方法接口说明

/login POST 发送登录请求

/logout POST 发送登出请求

/register POST 发送注册请求

/get/user GET 获取用户信息

/add/user POST 发送添加用户请求

/update/user POST 发送更新用户信息请求

/delete/user POST 发送删除用户请求

/userlog GET 获取用户日志

/system/deleteUserLog DELETE 发送删除用户日志请求

/system/getSystemInfo GET 获取系统资源利用率

/alarm/getAll GET 获取所有警报数据

/alarm/search GET 获取满足查询条件的警报数据

/alarm/getNextPage POST 根据总数据获取下一页数据

/alarm/classify GET 获取警报分类数据

/alarm/statistics GET 获取警报统计数据
/home/getResScore GET 获取威胁评分数据
/get/data/testattackgraph GET 获取传感器层攻击图数据
/get/data/getAttackgraphByStartEndPhy GET 获取传感器层攻击图源节点和目的节点间的攻击路径
/get/data/anotherAttackgraph GET 获取网络层攻击图数据
/get/data/anotherAttackgraphByFlag GET 根据 flag 获取网络层攻击图数据
/get/data/getAttackgraphByStartEndNet GET 获取网络层攻击图源节点和目的节点间的攻击路径
5. 系统实现
5.1 注册与登录
注册与登录页面是系统的入口。点击系统的网址，进入注册与登录页面，页面上方展示系统的名称，左侧展示一些经典工业控制系统的轮播图，右侧展示注册与登录的表单。 15
图5-1-1为系统注册页面的实现。
图 5-1-1 系统注册页面图5-1-2为系统登录页面的实现。
图 5-1-2 系统登录页面
5.2 系统主页
系统主页的布局如5-2-1所示，从上到下依次展示词云图、威胁评分折线图和警报数据表。威胁评分折线图循环播放主机在不同时间下的威胁评分。 16
图 5-2-1 系统主页
5.3 警报展示
警报数据展示页面主要展示基于警报数据的统计信息，包括攻击类型的数量随时间变化折线图、警报数量随时间变化折线图、攻击类型与攻击名称树状图和不同等级的警报数量扇形图。图表上方是搜索栏，用户可以输入开始时间、结束时间、源 IP 和目的 IP 来筛选警报数据来绘制图表。页面布局如图5-3-1所示。
17
图 5-3-1 警报数据展示页面攻击类型与攻击名称树状图设计如图5-3-2所示。初始展示攻击类型的种类，如图5-3-2a所示，点击具体攻击类型后展示该攻击类型对应的攻击名称，如图5-3-2b为攻击类型为 Misc Attack 的攻击名称树状图展示。
a) 攻击类型展示 b) Misc Attack 类型的攻击名称展示图 5-3-2 攻击类型与攻击名称树状图 18
5.4 攻击路径
攻击路径展示模块的实现分为传感器层攻击图的实现和网络层攻击图的实现，其具体介绍如下。
传感器层攻击图展示页面如5-4-1所示。页面左侧展示显示设置栏，可以点击按钮展示节点详情、固定节点位置、选择深度。页面右侧展示攻击场景信息，包括攻击图信息、节点详情、通过节点的攻击路径。
图 5-4-1 传感器层攻击图展示页面系统支持生成两点间的攻击路径，在左侧显示设置栏进行深度选择，选择起点、
终点，深度选择栏展示可选深度，用户选择深度，点击查询，生成该深度下的攻击路径。图5-4-2为 x1_low 到 x7_high 的深度为 5 的攻击路径展示。绿色节点代表起始节点，橙色节点代表终止节点。 19
图 5-4-2 x1_low 到 x7_high 的深度为 5 的攻击路径图网络层攻击图展示页面布局与传感器层相同，如图5-4-3所示。页面初始展示的攻击图仅包括设备节点和对应的边。
图 5-4-3 网络层攻击图展示页面点击两个设备节点之间的边，即可展示两个设备间的攻击节点，如图5-4-4所示。
红色节点为攻击节点。 20
图 5-4-4 网络层攻击图（展开一条边）
点击打开页面左侧显示设置中的显示全部滑块即可展示攻击图的全部节点，如图5-4-5所示。点击关闭该滑块即可收起攻击节点，仅展示设备节点与其对应的边。
图 5-4-5 网络层攻击图（显示全部）
在左侧显示设置栏进行深度选择，选择起点、终点，深度选择栏展示可选深度
（该深度为包含攻击节点的深度），用户选择深度，点击查询，生成该深度下的攻击路径。图5-4-6为设备节点 192.168.2.64 到设备节点 192.168.88.115 的深度为 5 的攻击路径展示。 21
图 5-4-6 节点 192.168.2.64 到节点 192.168.88.115 的深度为 5 的攻击路径图
5.5 数据管理
数据管理模块实现对警报数据的管理，页面主要展示每条警报数据信息，页面的左侧是搜索栏，可以输入开始时间、结束时间、类别、警报等级、攻击名称、源 IP、
目的 IP 和限制条数进行查询，类别、警报等级和攻击名称支持多选，查询出的警报
数据展示在页面右侧。页面布局如图5-5-1所示。
图 5-5-1 警报数据管理页面点击每条警报数据右侧的箭头，即可展示该条数据的详细信息，如图5-5-2所示。 22
图 5-5-2 单条警报数据展示
5.6 系统管理
系统管理模块的实现分为资源统计与用户管理两个部分，其具体介绍如下。
资源统计页面布局如图5-6-1所示。页面左侧展示用户登录登出日志信息表，右侧从上到下展示系统时间与系统资源的利用率。
图 5-6-1 资源统计页面用户管理页面根据用户权限（管理员/普通用户）展示不同，如图5-6-2所示。图5-
6-2a为管理员权限下的页面，页面展示用户信息表，通过点击相应的按钮，可以对用
户数据进行增、删、改、查等操作。图5-6-2b为普通用户权限下的页面，用户可以更改密码。 23
a) 管理员权限
b) 普通用户权限图 5-6-2 用户管理页面

6. 系统测试

软件测试是一种重要的质量保证手段，可以有效的验证系统的正确性、稳定性和可靠性，提升用户满意度[24]。因此，在系统代码完成时对系统进行软件测试至关重要。本节对工控网络攻击路径模拟与分析系统进行功能上和性能上的测试，以减少系统运行故障，提升用户的使用体验。测试的硬件、软件环境与 2.2 中环境相同，网络使用校园网，浏览器使用 Chrome 浏览器。

6.1 功能测试

对系统主要功能进行测试，其测试结果如表6-1-1所示。

24

表 6-1-1 功能测试表

功能名称功能描述测试结果

用户注册普通用户注册正确用户登录管理员、普通用户登录正确系统主页查看展示词云图、威胁评分折线图、警报数据表正确警报展示展示四张警报统计图正确攻击路径查看展示传感器层、网络层攻击图与对应的统计信息正确数据管理筛选并查看警报数据正确资源统计展示用户日志表与资源利用率正确用户管理管理员进行用户信息的增删改查，普通用户修改密码正确

1功能测试表格式参照论文面向测控系统的攻击路径分析系统设计与实现中表 5-3 [25]

对警报展示、攻击路径查看（传感器层/网络层）和数据管理三个核心模块的功

能进行重点测试，其测试结果如下。

警报展示模块的测试用例如表6-1-2所示。

表 6-1-2 警报展示模块测试用例表

编号测试内容预期结果测试结果

alarm1 开始时间大于结束时间提示对应报错信息正确

alarm2 所选时间范围不在有效时间范围内提示有效时间范围正确

alarm3 输入不合法 IP 提示 IP 格式错误正确

alarm4 输入错误的时间格式提示时间格式错误正确

alarm5 输入合法查询条件，查询统计图表四个统计图表展示无误正确

alarm6 输入空查询条件查询展示基于全部数据生成的统计图表正确传感器层攻击图展示模块的测试用例如表6-1-3所示。

25

表 6-1-3 传感器层攻击图展示模块测试用例表

编号测试内容预期结果测试结果

phy1 打开左侧节点详情开关攻击图节点旁显示节点名称正确

phy2 打开左侧固定位置开关攻击图节点固定正确

phy3 将鼠标悬停在节点上节点上方展示该节点的详情信息的提示框正确

phy4 在右侧节点详情选择节点查询展示该节点详情信息与通过的攻击路径正确

phy5 不选择起点，点击查询提示起点无效正确

phy6 不选择终点，点击查询提示终点无效正确

phy7 不选择深度，点击查询提示深度无效正确

phy8 选择起点、终点、深度，点击查询展示符合条件的攻击路径正确

phy9 点击清空刷新攻击图，重置深度选择栏正确网络层攻击图展示模块的测试用例如表6-1-4所示。

表 6-1-4 网络层攻击图展示模块测试用例表

编号测试内容预期结果测试结果

net1 打开左侧节点详情开关攻击图节点旁显示节点名称正确

net2 打开左侧固定位置开关攻击图节点固定正确

net3 打开左侧显示全部开关展示包含漏洞节点的整张攻击图正确

net4 将鼠标悬停在节点上节点上方展示该节点的详情信息的提示框正确

net5 点击两个设备节点间的边展示这两个节点间的漏洞节点正确

net6 在右侧节点详情选择节点查询展示该节点详情信息正确

net7 不选择起点，点击查询提示起点无效正确

net8 不选择终点，点击查询提示终点无效正确

net9 不选择深度，点击查询提示深度无效正确

net10 选择起点、终点、深度，点击查询展示符合条件的攻击路径正确

net11 点击清空刷新攻击图，重置深度选择栏正确数据管理模块的测试用例如表6-1-5所示。 26

表 6-1-5 数据管理模块测试用例表

编号测试内容预期结果测试结果

manage1 开始时间大于结束时间提示对应报错信息正确

manage2 输入不合法 IP 提示 IP 格式错误正确

manage3 输入错误的时间格式提示时间格式错误正确

manage4 输入不合法限制条数提示限制条数需为大于 0 的整数正确

manage5 输入合法查询条件，查询警报数据展示该条件下的警报数据正确

manage6 输入空查询条件，点击查询展示全部警报数据正确

manage7 点击单条警报数据右侧箭头展示该条数据详情信息正确

测试分析结果表明，该系统能够正确的完成核心模块的功能，并且符合预期的结

果。

6.2 性能测试

本文对系统的性能进行了测试，测试了不同页面数据加载与请求响应速度，测试

结果表明，除了数据管理页面加载速度较慢（约为 1 至 2 秒）以外，系统的其他页面

均可以在 1s 内加载完成。值得一提的是，按照深度对两个节点间的攻击路径搜索请求响应很快，在选择了起点与终点后，深度搜索栏可以快速展示可选深度值，且点击查询之后，可以几乎无卡顿展示攻击路径图，这得益于数据表 NetPathGraph 的设计与路径查询算法的优化（表4-2-12）。

本系统成功的通过了性能测试的基本要求，在大部分页面的测试中表现良好，但是部分页面的加载仍然具有较大的提升空间，例如，警报数据管理页面的响应时间需要 1 至 2s，经过测试发现，该页面的后端接口响应速度并不慢，且前端页面加载速度与接口返回的数据量有关，数据量越大，页面加载越慢，因此，可以考虑对前端代码进行优化，提高页面的加载速度。

7. 总结

基于警报数据的攻击路径生成与分析是当前工控网络安全防护领域的一个热点问题。未来，随着工控网络的发展与技术的革新进步，其遭受的网络安全威胁也在增加与升级。对工控网络中的攻击路径的模拟、分析与可视化的研究具有重要意义，可视化的形式使攻击图信息更直观的呈现，可以更好的辅助工控网络安全保护与防御 27

工作。

本文设计并实现了一个基于警报数据的工控网络攻击路径模拟与分析系统，实现了警报数据的管理、分析与展示的功能，处理警报数据，动态生成并展示攻击路

径，并生成对攻击路径的分析结果。通过可视化的手段，将复杂的攻击图数据以图形

化的方式呈现给用户，能够更加直观、形象地展示攻击过程，易于分析和理解。

测试表明，本系统顺利达成了既定的目标，完成了基本的功能性需求，但是仍然

存在一些缺陷。例如，某些页面加载缓慢、搜索数据返回结果较慢、对攻击图的分析

方法比较简单等问题。这些问题会影响用户体验，因此需要进一步优化系统性能，深入挖掘攻击图信息，提升系统的可用性和用户满意度。同时，要结合人工智能和大数据技术，不断完善攻击路径预测和响应机制，为工控网络的安全发展提供更加有力的支持。 28

参考文献

[1] 杨伟, 周权. 工业控制系统安全及对策[J]. 信息安全与技术, 2018, 009(007): 60-63, 73.

[2] KUSHNER D. The real story of stuxnet[J]. IEEE Spectrum, 2013, 50(3): 48-53.

[3] LIANG G, WELLER S R, ZHAO J, et al. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks[J]. IEEE Transactions on Power Systems, 2017, 32(4): 3317-3318.

[4] AKBANOV M, VASSILAKIS V G, LOGOTHETIS M D. Ransomware detection and mitigation using software-defined networking: The case of WannaCry[J]. Computers & Electrical Engineering, 2019, 76: 111-121.

[5] 王得金, 江常青, 彭勇. 工业控制系统上基于安全域的攻击图生成[J]. 清华大学学报 (自然科学版), 2014, 54(1): 44-52.

[6] 吴迪, 连一峰, 陈恺, 等. 一种基于攻击图的安全威胁识别和分析方法[J]. 计算机学报, 2012, 35(9): 1938-1950.

[7] 陈锋, 张怡, 苏金树, 等. 攻击图的两种形式化分析[J]. 软件学报, 2010(4): 838-848.

[8] BARIK M S, MAZUMDAR C. A Graph Data Model for Attack Graph Generation and Analysis[C]//MARTÍNEZ PÉREZ G, THAMPI S M, KO R, et al. Recent Trends in Computer Networks and Distributed Systems Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014: 239-250.

[9] FENG Y, SUN G, LIU Z, et al. Attack Graph Generation and Visualization for Industrial Control Network[C]//2020 39th Chinese Control Conference (CCC). 2020: 7655-7660.

[10] WILLIAMS L, LIPPMANN R, INGOLS K. An Interactive Attack Graph Cascade and Reachability Display[M]//GOODALL J R, CONTI G, MA K L. VizSEC 2007: Proceedings of the Workshop on Visualization for Computer Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 221-236.

[11] ZENITANI K. Attack graph analysis: An explanatory guide[J]. Computers & Security, 2023, 126: 81-103.

[12] 贺军. 浅谈网络安全攻防技术[J]. 环球市场, 2020, 000(029): 383.

[13] WANG C, DU N, YANG H. Generation and Analysis of Attack Graphs[J]. Procedia Engineering, 2012, 29: 4053-4057. 29

[14] FENG Y, SUN G, LIU Z, et al. Attack Graph Generation and Visualization for Industrial Control Network[C]//2020 39th Chinese Control Conference (CCC). 2020: 7655-7660.

[15] PHILLIPS C, SWILER L P. A Graph-Based System for Network-Vulnerability Analysis[C]//NSPW '98: Proceedings of the 1998 Workshop on New Security Paradigms. Charlottesville, Virginia, USA: Association for Computing Machinery, 1998: 71-79.

[16] OU X, GOVINDAVAJHALA S, APPEL A W. MulVAL: A Logic-based Network Security Analyzer[C]//14th USENIX Security Symposium. Baltimore, MD: USENIX Association, 2005: 113-128.

[17] LIPPMANN R, INGOLS K, SCOTT C, et al. Validating and Restoring Defense in Depth Using Attack Graphs[C]//MILCOM 2006 - 2006 IEEE Military Communications conference. 2006: 1-10.

[18] 叶子维，郭渊博，王宸东，等. 攻击图技术应用研究综述[J]. 通信学报，2017，38(11)：12.
[19] 徐丽娟. 基于攻击图的工业控制网络安全隐患分析[D]. 北京邮电大学，2015.
[20] 黄家辉，冯冬芹，王虹鉴. 基于攻击图的工控系统脆弱性量化方法[J]. 自动化学报，2016，42(5)：7.
[21] FADLALLAH A，SBEITY H，MALLI M，et al. Application of Attack Graphs in Intrusion Detection Systems: An Implementation[J]. International Journal of Computer Networks，2016，8(1)：1-12.
[22] AHMADINEJAD S H，JALILI S，ABADI M. A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs[J]. Computer Networks，2011，55(9)：2221-2240.
[23] 刘威歆，郑康锋，武斌，等. 基于攻击图的多源告警关联分析方法[J]. 通信学报，2015，36(9)：10.
[24] 张新华，何永前. 软件测试方法概述[J]. 科技视界，2012.
[25] 张耀方. 面向测控系统的攻击路径分析系统设计与实现[D]. 哈尔滨工业大学，2021. 30

致谢

值此本科毕业论文完成之际，我要向所有关心、支持和帮助过我的人们致以最真挚的感谢！

首先，我要感谢我的导师宋轩老师。在我完成毕业论文的过程中，给予了我无私的指导和帮助，让我在学术上有了更深入的理解，并且能够以更系统、更科学的方式来研究我的课题。您的悉心培养和耐心指导，对我今后的学习和工作都将产生巨大的影响。

同时，我还要感谢指导我完成毕业设计的赵奕丞师兄、马琦师兄与张耀方师姐，无论是在学业上，还是在生活中，你们耐心的指导、帮助与鼓励让我受益匪浅，而且更加坚定了我实现自己理想的决心。

最后，我还要感谢我的同学和朋友们。我将永远铭记你们的友情和支持，在人生的道路上一直与你们共同努力前行。

感谢有你们，我才能在本科生活的四年间不断成长，收获的不仅是知识，还有珍贵的人生经验。最后，再次向各位致以衷心的感谢！ 31