**《网络被攻击过程图形化显示系统》**

**概要设计说明书**

**修订表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **版本** | **修订人** | **修订章节与内容** | **修订日期** |
| 1 | 1.0 | 张海汀 | 初版概要设计说明书 | 2020/9/12 |
| 2 | 1.1 | 张海汀 | 补充模块设计和数据结构部分 | 2020/9/13 |
| 3 | 1.2 | 张海汀 | 调整“容灾设计”并增加“风险预期及应对”部分 | 2020/9/14 |
| 4 | 1.3 | 张海汀 | 修改界面设计、数据结构 | 2020/9/16 |
|  |  |  |  |  |

**目录**

一、引言

1.目的

2.范围

二、总体设计

三、外部接口

四、模块设计

五、数据结构

1.逻辑结构

2.物理结构

六、容灾设计

七、用户界面设计

八、风险预测及应对

九、其他

附录：制定规范

代码规范

一、引言

1.目的

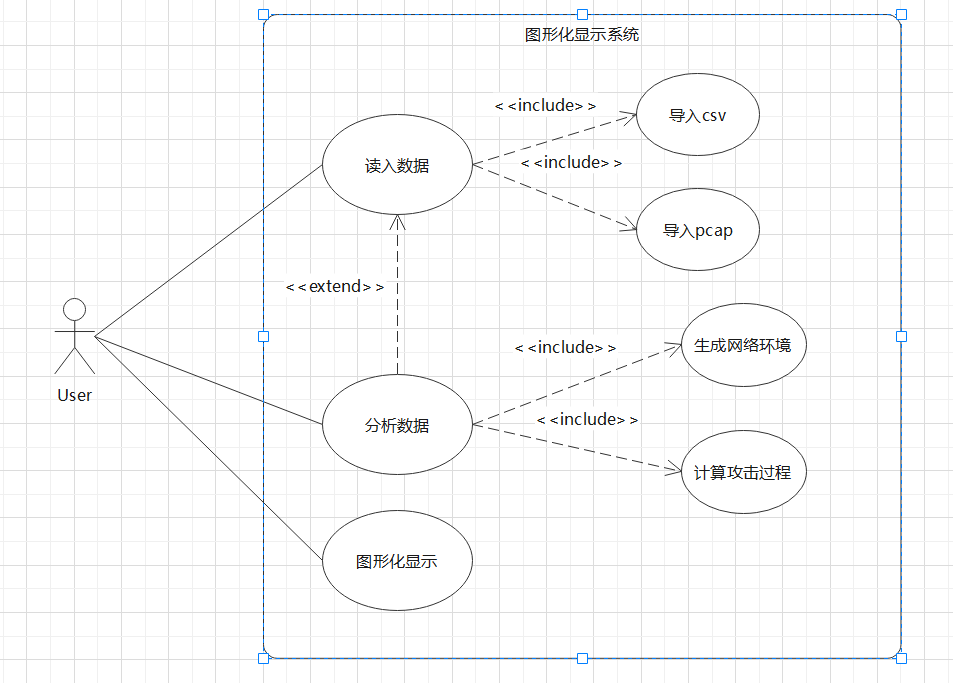
本文档为网络被攻击过程图形化显示系统的概要设计说明书，根据《网络被攻击过程图形化显示系统需求规格说明书》中规定的需求而编写，旨在明确说明系统各个功能的实现方式，以作详细设计和系统实现的依据。

2.环境

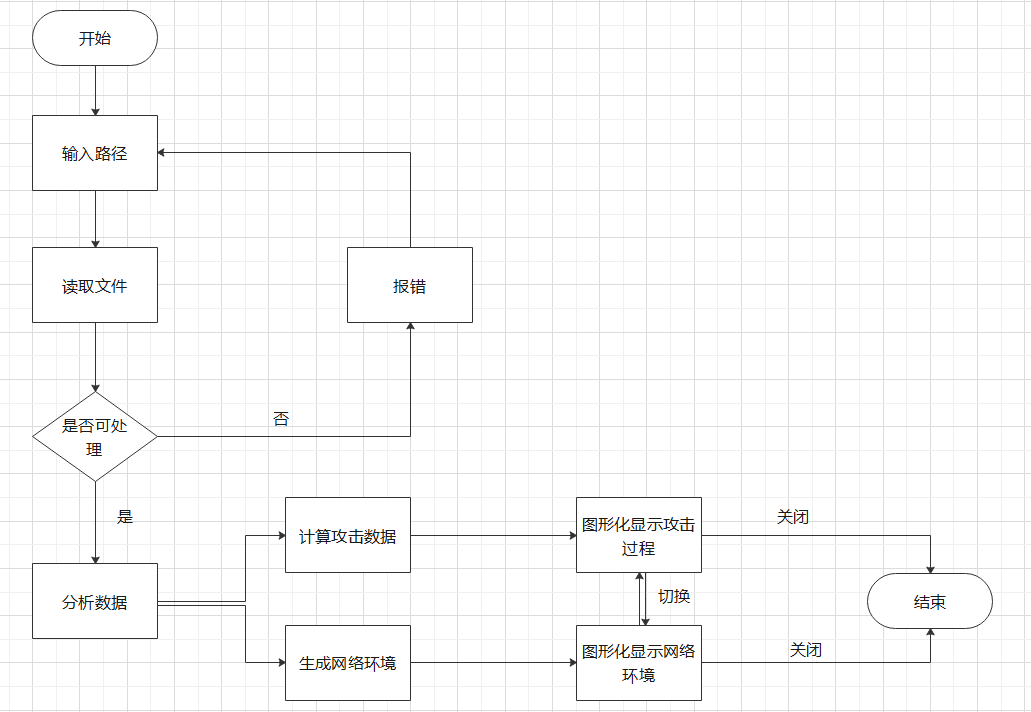
Windows 10计算机系统。

二、总体设计

1.用例图

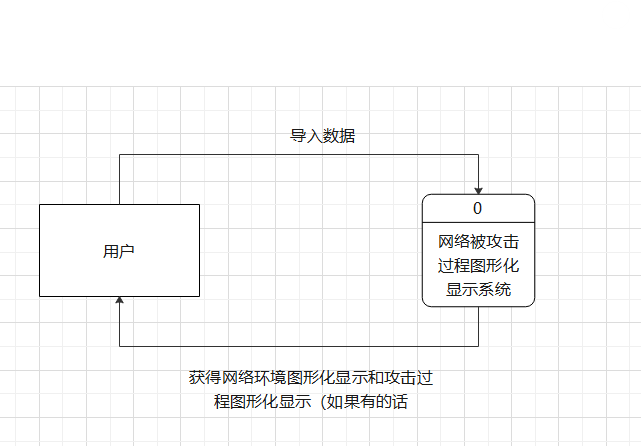


2.系统流程图

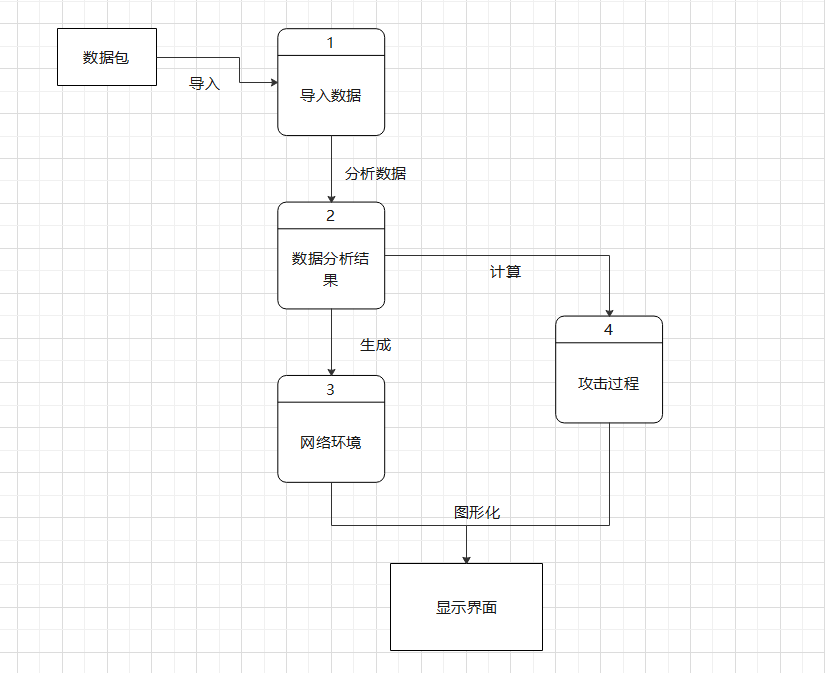


3.数据流图

3.1 上下文图



3.2 0层图



三、外部接口

本系统不需要与其他系统对接，所以无外部接口。

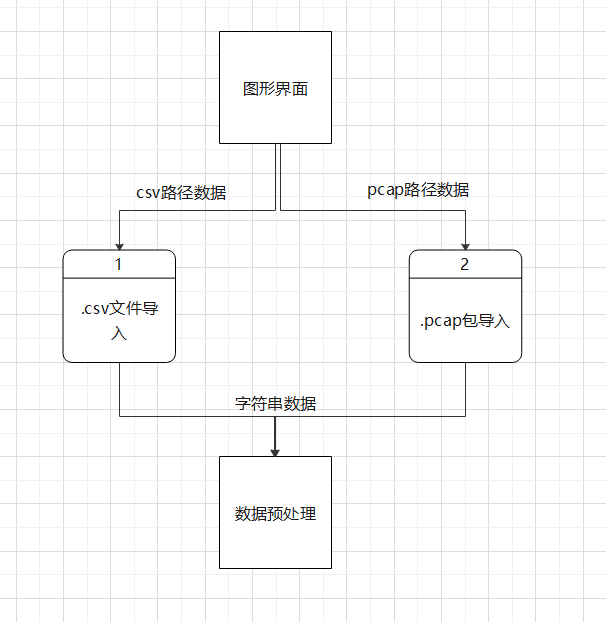
四、模块设计

1.导入数据模块

1.1 导入.csv文件

1.2 导入.pcap数据包

1.3 1层图



2.分析数据

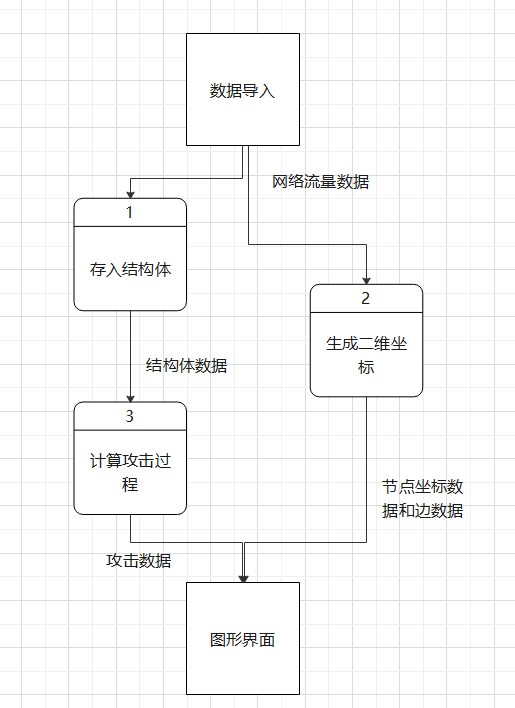
2.1 数据预处理

包括根据IP生成前端需要的二维坐标、将需要的数据部分存入结构体以便于后续计算。

2.2 计算攻击过程

2.3 数据交互

2.4 1层图



3.图形化显示

3.1 面向后端的接口

3.2 初始界面和获取用户输入

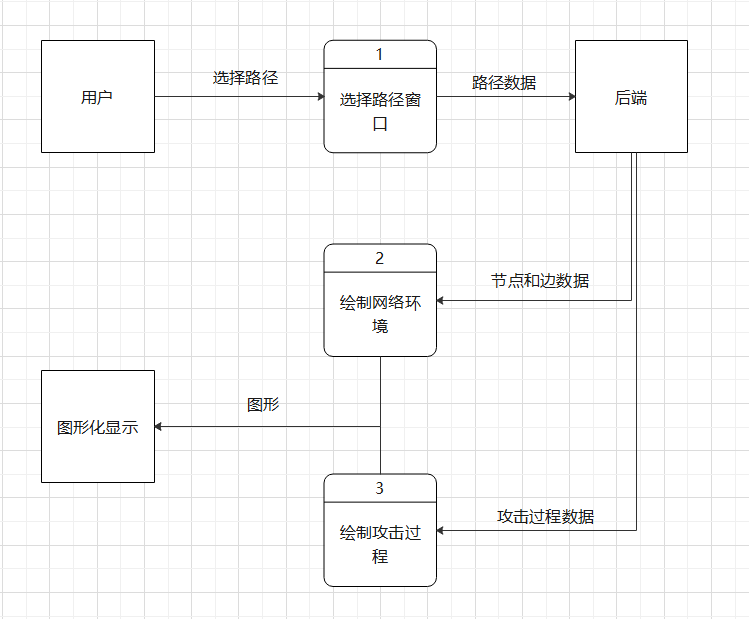
3.3 显示网络环境

包括限制时间范围、节点分类显示、放大缩小等需求。

3.4 显示攻击过程

包括限制时间范围、节点分类显示、放大缩小、显示指定攻击等需求。

3.5 1层图



五、数据结构

1.逻辑结构

~~后端内部使用类(class)的逻辑结构，用于临时存储数据，便于计算攻击过程。~~

使用类构成两条单链表。一条作为存储节点，在链表头新建一节存储节点，定时扫描链表并删除过期的节点；一条用于存储边，在链表头新建一节存储边，定时扫描链表并删除过期的边。

2.物理结构

由系统自动分配。

六、容灾设计

我们采用QQ群文件和GitHub仓库进行双重云端备份内容，完成的文档和代码及时上传至QQ群文件并每日一次将所有代码和文档更新上传至GitHub，能够有效减轻“电脑丢失”或“云端数据库故障”等灾难事件带来的损失。

我们的GitHub仓库链接为：

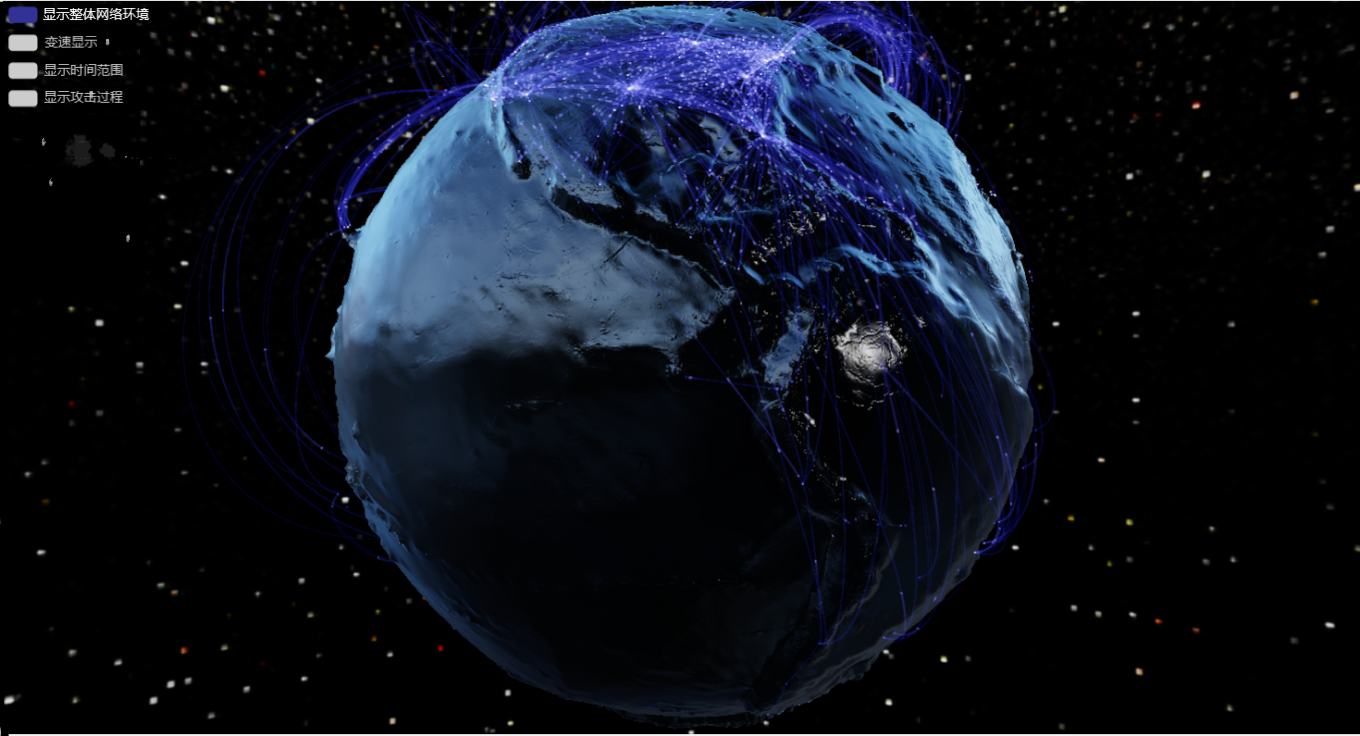
https://github.com/Cheeennnnnnnn/Unnamed

七、用户界面设计

1.初始界面

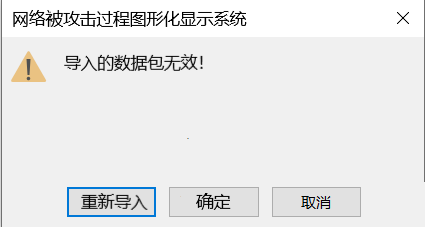
（待补充

2.网络环境图形化显示界面



3.数据包报错设计

报错时弹出消息框提示数据包不可用。



八、风险预测及应对

1.前端部分风险分析及应对方案

1. 1风险分析

1）我们全组对于前端需要的架构手段不熟悉，可能需要过量的时间进行查阅资料和学习使用。

2）我们是第一次使用这种前端架构，不确定这种架构能否满足我们所有的需求——或者我们可能时间范围内不能学会如何使用这种架构完成我们的部分需求。

1.2 应对方案

1）开始编码前适当加班学习。

2）放弃部分非核心功能的需求。

2.后端部分风险分析及应对方案

2.1 风险分析

1）数据量过大，可能程序不能达到性能需求。

2）很多攻击过程难以计算，可能除了DOS攻击以外的攻击过程都算不出来。

3）从未进行过如此大数据量的拓补图生成，可能做不出来。

4）单位时间内数据过多，无法按时完成读取和显示。

2.2 应对方案

1）加班和查阅资料，如果没有办法，放弃部分性能需求。

2）加班和查阅资料，如果时间和人力不足，放弃部分攻击种类的计算。

3）加班。

4）弹出数据量过大的报错和攻击发生预警。

3.测试部分风险分析及应对方案

3.1风险分析 \*来源：测试计划

1）项目完成时间比较紧迫的风险：由于整个项目从立项到最后完成交付的时间只有 3 周，所以有可能没有时间将所以的测试计划都按时执行、或者有的测试方面没有覆盖到。

2）测试工具使用的风险：由于该项目的所涉及到的主题：网络攻击过程图，是我们小组成员之前所没有涉及到的知识领域，所以对与之有关的测试工具可能使用经验不足，需要花费一定的时间研究。

3.2 应对方案

1）根据项目现状，可能需要适当放弃部分与功能需求关系不够密切的部分的测试计划。

2）前期做足准备，如果有需要的话适当加班。

九、其他

暂无。

附录：制定规范

代码规范

