东南大学 SOUTHEAST UNIVERSITY
网络空间安全学院 School Of Cyber Science and Engineering

# 面向事件属性的扫描意图分析

汇报人：黄勉

2023年11月30日

# 目录

# 研究背景

## 扫描意图

- 扫描行为具备不同的**意图**
- 观测并研究扫描意图，有助于掌握网络环境，识别攻击前兆

| 扫描主体 | 扫描目的 | 扫描意图 |
| --- | --- | --- |
| 网络测绘机构 | 研究或监测安全情况 | 非恶意 |
| 网络管理员 | 发现网络漏洞，确保系统安全 | |
| 普通用户 | 查找网内可用资源，出于兴趣或练习目的 | |
| 黑客 | 选择攻击目标，为攻击做准备 | 恶意 |

扫描主体及扫描意图

# 目录

# 扫描流量的获取

## IBR流量

互联网背景辐射(Internet Background Radiation，简称 IBR)流量是指**未经请求的单向流量**，是进行扫描相关研究的**理想数据源**

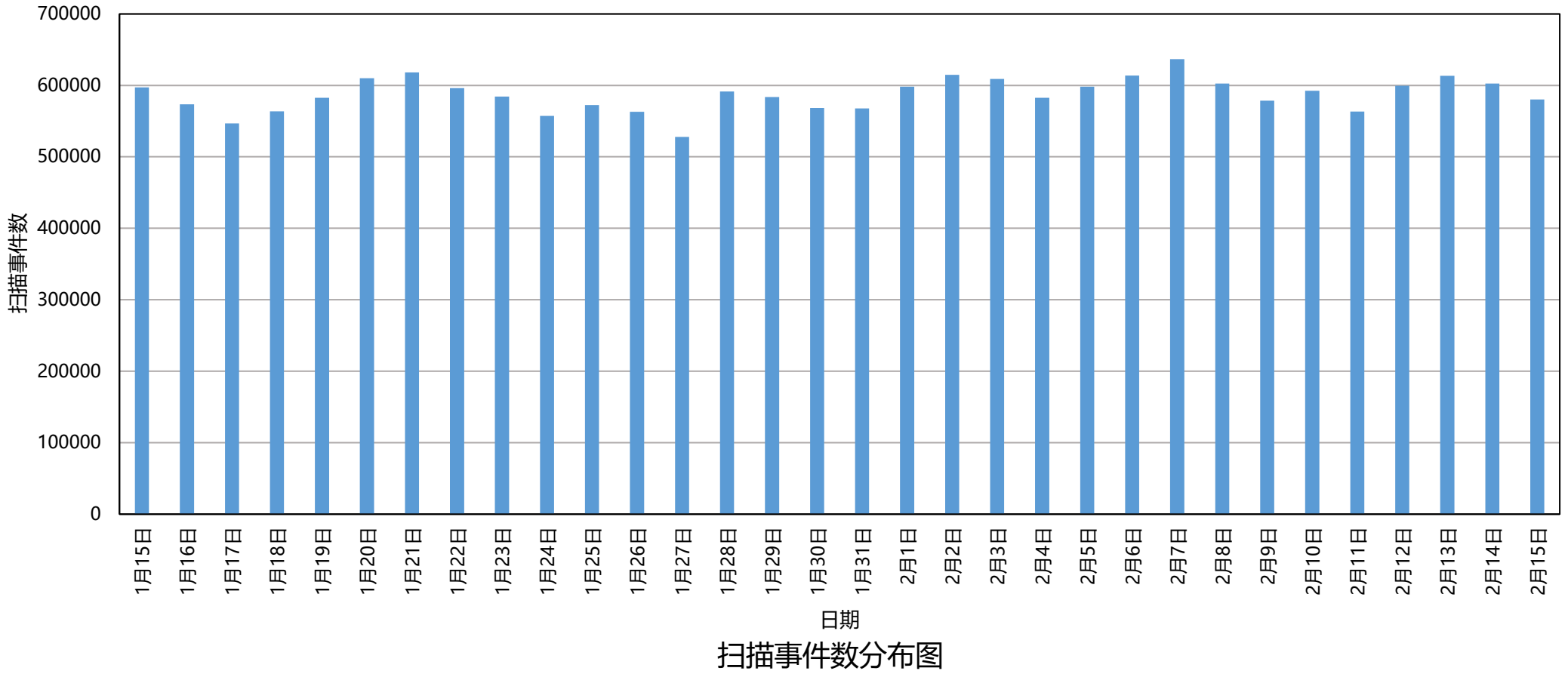
## 扫描流量

**TCP 扫描报文：**带有 TCP SYN标志位的报文

**UDP扫描报文：**建立UDP常用应用协议请求报文有限状态自动机，对UDP扫描报文进行识别

# 扫描事件

**扫描事件定义：** 对于一个**给定源地址**在连续时间**(t)**内发出的扫描流量，如果扫描对端IP数大于给定的数量阈值**(N)**，则称这些扫描流量的集合为一个扫描事件




扫描事件数分布图

# 扫描事件属性

### 扫描事件容量
一个TCP/UDP扫描事件所检测到的所有扫描报文数

### 扫描事件协议数
一个UDP扫描事件中所有已识别UDP协议数目

### 扫描事件端口数
一个 UDP扫描事件扫描的所有端口数目

### 扫描事件报文压缩比
一个UDP扫描事件去除重复扫描的报文数量与整个扫描事件报文总数的比例

### 全网扫描
一个UDP扫描事件扫描的地址空间

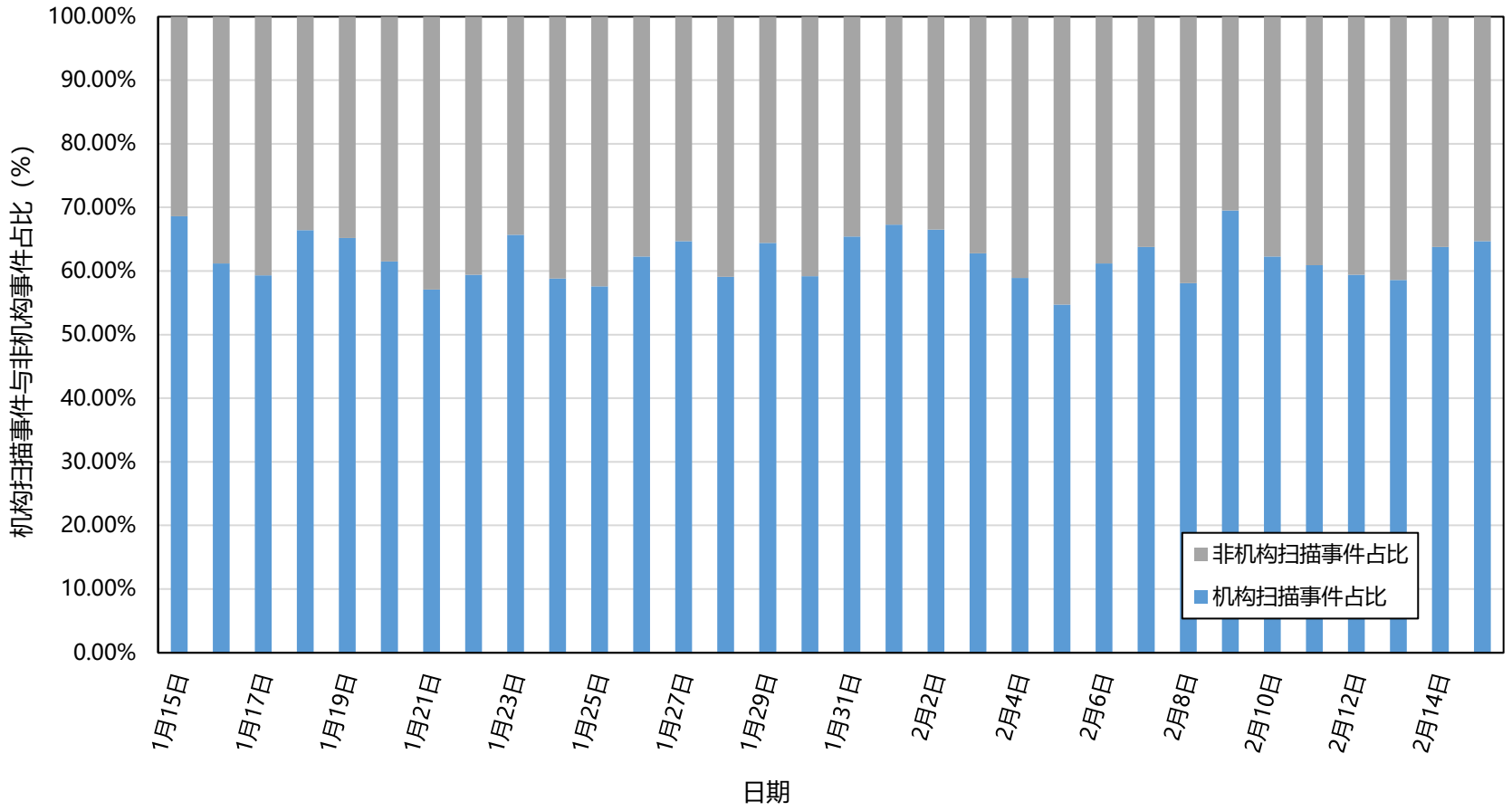
### 扫描事件归属
一个 UDP扫描事件的扫描源地址归属机构

# 扫描事件归属属性

| 扫描机构 | 机构网站 | 机构角色 | 机构扫描源地址数 |
| --- | --- | --- | --- |
| University of Michigan | ces.engin.umich.edu | 研究院校 | 1524 |
| Censys | censys.io | 商业机构 | 1270 |
| Rapid7 | opendata.rapid7.com | 商业机构 | 374 |
| NETSCOUT | www.arbor-observatory.com | 研究院校 | 254 |
| Qrator Labs | qrator.net | 商业机构 | 254 |
| Shadowserver Foudation | www.shadowserver.org | 商业机构 | 242 |
| ONYPHE | www.onyphe.io | 商业机构 | 148 |
| Net Systems Reseach | www.netsystemseach,com | 研究机构 | 146 |
| IPIP.NET | IPIP.NET | 商业机构 | 126 |
| Internet Census Group | www.internet-census.com | 商业机构 | 80 |
| Shodan | shodan.io | 商业机构 | 45 |
| Stretchoid | stretchoid.com | 商业机构 | 24 |
| InternetTTL | www.intenetttl.org | 研究机构 | 19 |
| Criminal IP | security.criminalip.com | 商业机构 | 14 |
| Cybergreen | www.cybergreen.net | 公益机构 | 12 |
| Georgia Institute of Technology | sarosi.artrolavos.gatech.edu | 研究院校 | 4 |
| University of Twente | research.openresolve.rs | 研究院校 | 1 |
| Delft University of Thnlogy and Grenoble Instittute of Technology | or.mkorczynski.com | 研究院校 | 1 |

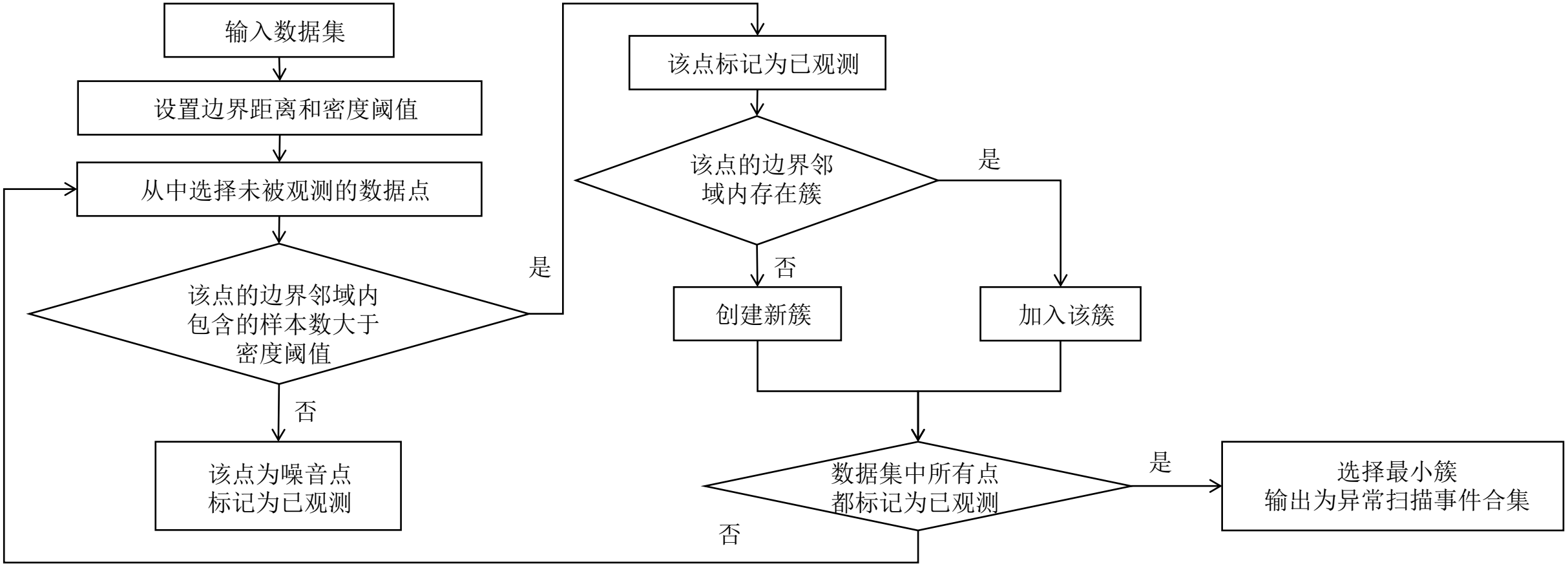
机构扫描源地址统计情况

# 机构扫描事件




机构扫描事件占比图

# 基于 DBSCAN 的异常扫描事件检测




基于DBSCAN的扫描事件异常检测算法流程图

# 参数设置

## 评价指标：轮廓系数

$$\begin{cases} S = \dfrac{1}{N} \times \sum_{j=1}^{N} S(i)\,;\ S(i) = \dfrac{b(i) - a(i)}{\max\{a(i),\ b(i)\}}; \\ b(i) = \min\left\{ \dfrac{1}{|C_j|} \sum_{l \in C_j} d(i,\ l) \right\} \qquad (j = 1,\ 2, \cdots,\ N \text{ 且 } j \neq k) \end{cases}$$

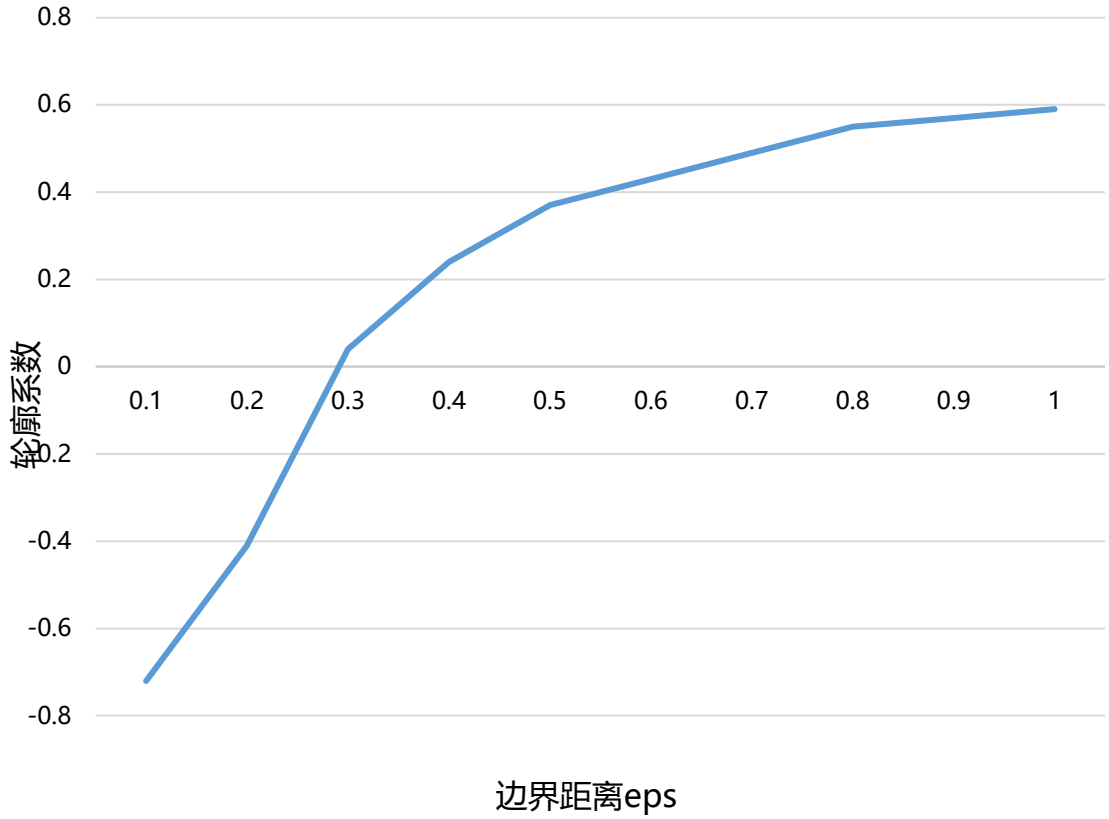
## 参数设置

边界距离设置为0.8

密度阈值设置为15

## 聚类特征

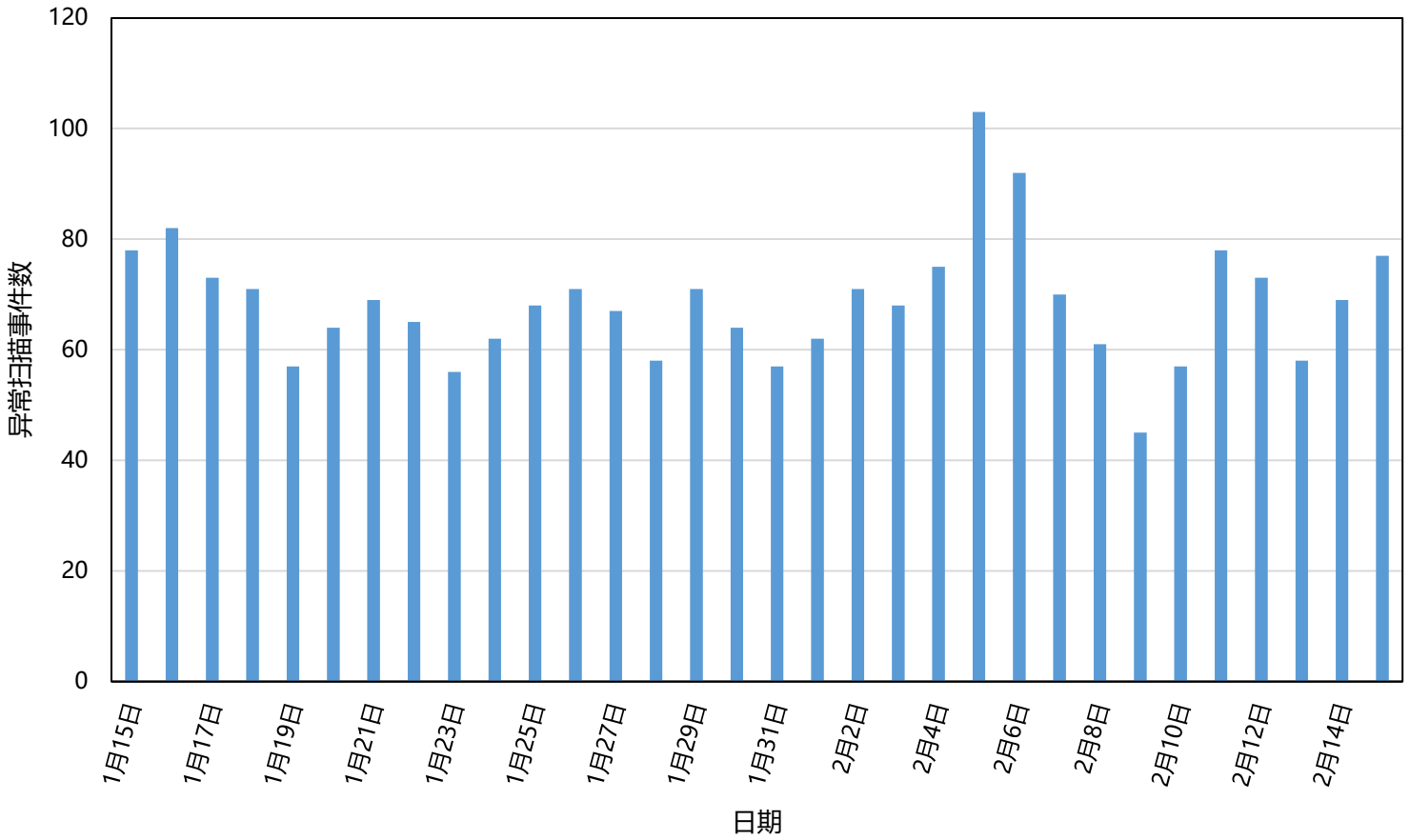
除扫描事件归属以外的五个扫描事件属性




轮廓系数与边界距离eps的关系

# 目录

# 实验结果




异常扫描事件分布图

# 实验结果

## 异常扫描事件验证

| 判别类别 | 潜在异常扫描事件数 |
| --- | --- |
| 正报数 | 29 |
| 误报数 | 13 |
| 无法判别 | 3 |
| 合计 | 45 |

2023 年 2 月 9 日异常事件正误报情况

| 扫描后续意图 | 异常扫描事件数 |
| --- | --- |
| 暴力攻击 | 17 |
| 恶意主机端口扫描 | 8 |
| 洪水查询 | 3 |
| 后门利用 | 1 |

2023 年 2 月 9 日正报异常扫描事件分布情况

# 目录

# 总结与展望

## 总结

提出扫描事件的定义

提出6个维度的属性对扫描事件进行描述

提出1种异常扫描事件检测方法

## 展望

对于扫描事件的属性可以进一步的扩充

对于检测出的异常扫描事件可以采取进一步措施

# 谢谢大家

**汇报人：黄勉**

2023年11月30日