

**2021年秋季学期  
计算学部《软件安全》**

**Lab5实验报告**

|  |  |
| --- | --- |
| 姓名 | 余涛，崔同发 |
| 学号 | 1180300829，1180300801 |
| 专业 | 信息安全 |
| 班号 | 1803202 |
| 手机号码 | 15586430583 |

## 1、实验项目描述

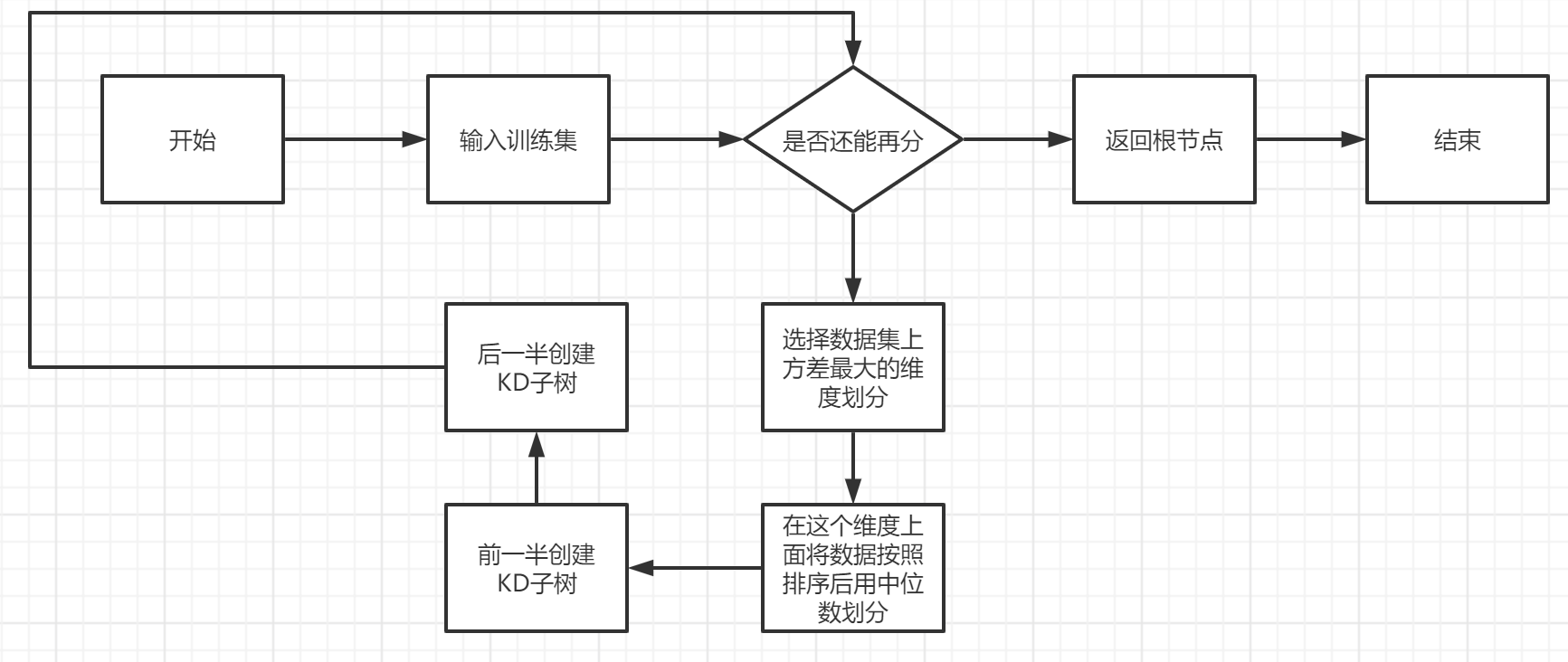
1. 理解基于异常检测的恶意攻击行为检测方法
2. 掌握异常检测的流程
3. 学习相关的异常检测算法
4. 基于距离的异常检测方法
5. 掌握欧氏距离的概念
6. 如何选取数据集的属性集
7. 选取合适的检测模型
8. 基于KD树的网络流量异常检测模型
9. 利用KD树构建一个用于多维空间最邻近搜索的数据结构
10. 建立历史数据集合
11. 规格化数据
12. 采用标准分割策略，进行基于维度分割的KD树构建
13. 基于待检测数据X，利用构建好的KD树搜索，找出历史数据集合中与待检测数据X最近的数据；计算二者之间的欧氏距离，与阈值比对，确定是否是异常数据点。

## 2、实验要求

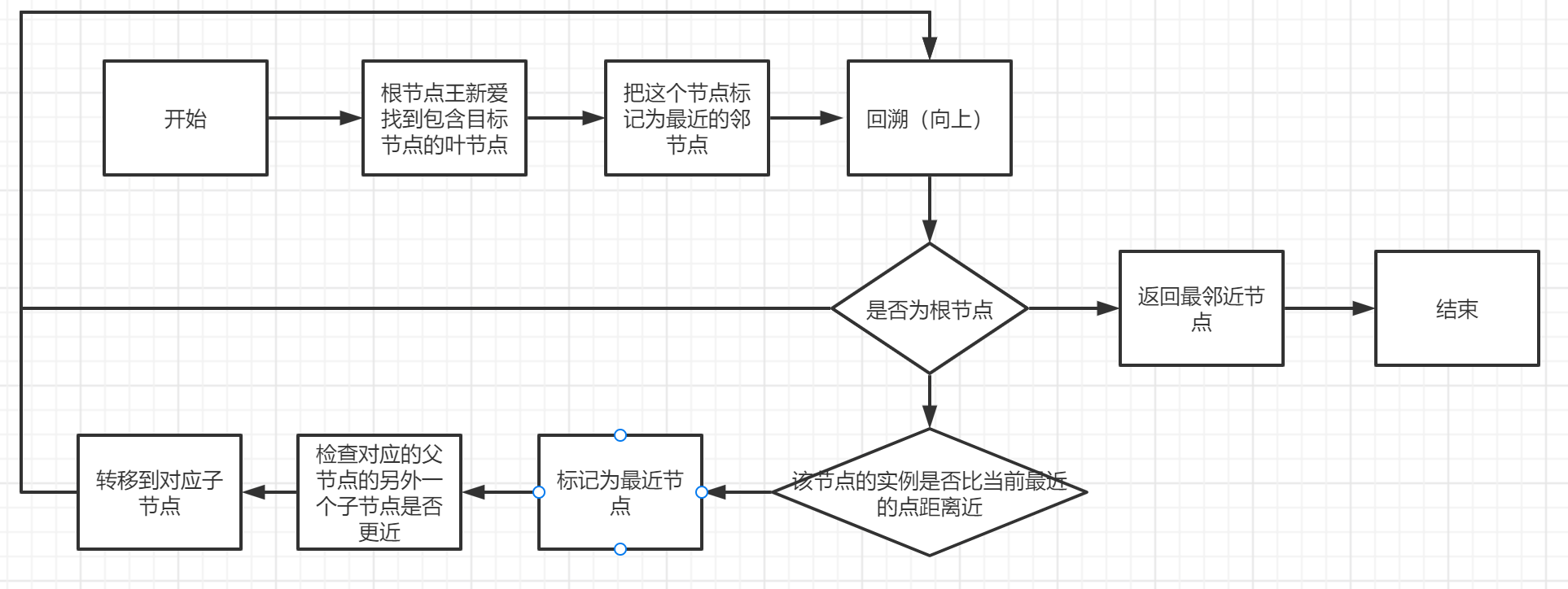
1. 实验数据准备。利用KDD1999数据集(KD树异常检测.pdf p31页-34页)提供的数据进行实验。选取部分正常数据做为训练集，选择部分攻击数据和剩下的正常数据做为测试集。
2. 可以只选择流量属性集(KD树异常检测.pdf p34页)。可只针对DOS(smurf攻击即可)攻击进行异常检测，其他攻击不考虑。
3. 2人一组完成实验。
4. 下载阅读 “实验5相关资料”中的KD树异常检测.pdf文件
5. 利用 “实验5相关资料”中的kdd原始数据中的kddcup.data\_10\_percent作为数据（看数据说明）。数据中每条都有标记为：NORMAL 或 ATTACK 类型。利用标记为 NORMAL 的数据建模（构建KD树）。利用一部分标记为 NORMAL 的数据 和ATTACK数据作为测试数据。 （数据集中可能存在少量有错误的数据，注意）

## 3、实验结果

1、创建KD树：



2、在KD树上面搜索最近邻



3、数据结构：

class KD\_node:

def \_\_init\_\_(self, point = None, split = None, left = None, right = None):

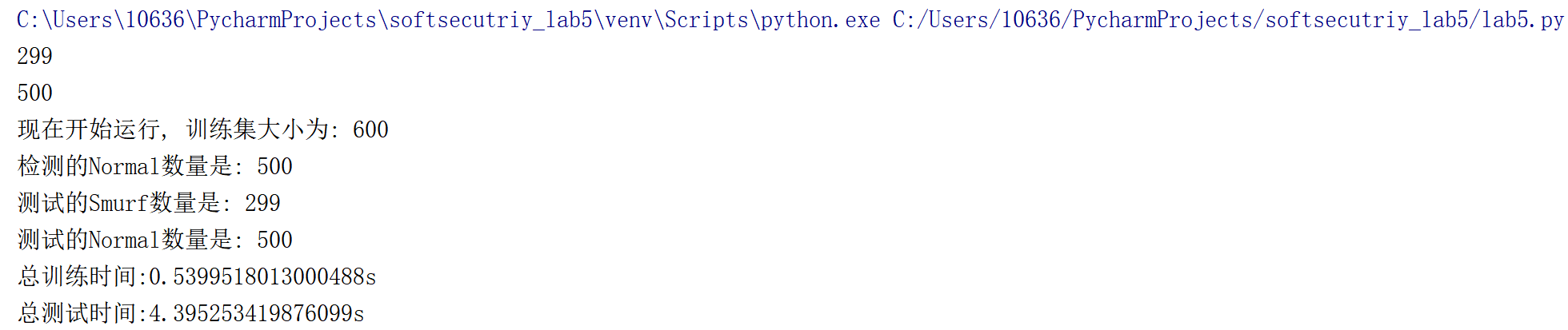
self.point = point # 数据点的特征向量

self.split = split # 切分的维度

self.left = left # 左儿子

self.right = right # 右儿子

4.实验结果：



测试结果准确