进度：

1.确定实验的数据集为NIDS数据集。

该数据集有v1，v2两个版本。打算采用v1版本作为毕设的数据集。因为v1版本与目前科技网的netflow流量字段较为相似。V2版本包含应用负载的相关特征，暂时无法落地应用

2.搜集该数据集的相关研究进展

数据集发布于2021 年，较新，所以相关研究不多

3.初步选择实验方向

数据集不包含流时间特征，所以无法基于时序异常检测的思路来做

基于流量异常的相关研究可以发现两点不足：

1. 目前大多流量异常检测采用的是监督学习，同时使用了正常和异常的流量数据来训练模型。但是在实际网络环境中，网络攻击方式多样，更新迭代快，未知的攻击流量占据了大多数，这时监督学习的方式就难以保证能够准确的区分出正常和异常流量。
2. NIDS数据集的v2版本的相关实验的准确率非常高，但是v1版本因为特征少，目前的相关研究准确率并不高，有提升空间。因为v1实用性更大，所以具有研究意义

基于两点不足可以总结两个研究方向：

1. 基于无监督学习训练模型，可以采用像自编码器算法只使用正常流量来训练模型，这样即使遇到新型的网络流量攻击也能够识别。这部分可以对应课题的第一个部分：流量异常发现。
2. 在特征数不足的情况下，如何提高流量分类的准确性。这部分可以对应课题的第二个部分：流量分类。

后续计划：

采用自编码器算法应用于数据集，测试效果。

自编码器参考资料：

[[1802.09089] Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection (arxiv.org)](https://arxiv.org/abs/1802.09089)

<https://blog.csdn.net/weixin_47160526/article/details/123683457>

<https://zhuanlan.zhihu.com/p/260882741>

# NIDS

## 数据集

### 数据源

NIDS数据集地址：

<https://staff.itee.uq.edu.au/marius/NIDS_datasets/#RA1>

论文地址：

<https://doi.org/10.1007/978-3-030-72802-1_9>

### 数据集标签

#### NF-UNSW-NB15

| 类别 | 数量 | 描述 |
| --- | --- | --- |
| Benign | 1550712 | 正常流 |
| Fuzzers | 19463 | 攻击者发送大量随机数据导致系统崩溃，并旨在发现系统中的安全漏洞。 |
| Analysis | 1995 | 一个通过端口、电子邮件和脚本呈现针对 Web 应用程序的各种威胁的组。 |
| Backdoor | 1782 | 一种旨在通过回复特定构造的客户端应用程序来绕过安全机制的技术。 |
| DoS | 5051 | 拒绝服务是指试图使计算机系统的资源过载，目的是阻止对其数据的访问或可用性。 |
| Exploits | 24736 | 是通过已知漏洞控制主机行为的命令序列 |
| Generic | 5570 | 一种以密码学为目标并导致与每个分组密码发生冲突的方法。 |
| Reconnaissance | 12291 | 一种用于收集有关网络主机的信息的技术，也称为探测器。 |
| Shellcode | 1365 | 一种恶意软件，可渗透代码以控制受害者的主机。 |
| Worms | 153 | 自我复制并传播到其他计算机的攻击。 |

#### NF-ToN-IoT

| 类别 | 数量 | 描述 |
| --- | --- | --- |
| Benign | 270279 | 正常流 |
| Backdoor | 17247 | 一种旨在通过回复特定构造的客户端应用程序来攻击远程访问计算机的技术。 |
| DoS | 17717 | 试图使计算机系统的资源过载，目的是阻止对其数据的访问或可用性。 |
| DDoS | 326345 | 一种类似于 DoS 的尝试，但具有多个不同的分布式源。 |
| Injection | 468539 | 提供不受信任的输入以改变执行过程的各种攻击，其中 SQL 和代码注入是其中两个主要的攻击。 |
| MITM | 1295 | Man In The Middle 是一种将攻击者置于受害者和受害者试图与之通信的主机之间的方法，目的是拦截流量和通信。 |
| Password | 156299 | 涵盖了旨在通过暴力破解或嗅探检索密码的各种攻击。 |
| Ransomware | 142 | 一种对存储在主机上的文件进行加密并要求补偿以换取解密技术/密钥的攻击。 |
| Scanning | 21467 | 由各种技术组成的组，旨在发现有关网络和主机的信息，也称为探测。 |
| XSS | 99944 | 跨站点脚本是一种注入类型，攻击者使用 Web 应用程序向最终用户发送恶意脚本。 |

#### NF-BoT-IoT

| 类别 | 数量 | 描述 |
| --- | --- | --- |
| Benign | 13859 | 正常流 |
| Reconnaissance | 470655 | 一种用于收集有关网络主机的信息的技术，也称为探测器。 |
| DDoS | 56844 | 分布式拒绝服务是一种类似于 DoS 的尝试，但具有多个不同的分布式源。 |
| DoS | 56833 | 试图使计算机系统的资源过载，目的是阻止对其数据的访问或可用性。 |
| Theft | 1909 | 旨在获取敏感数据（例如数据盗窃和键盘记录）的一组攻击 |

#### NF-CSE-CIC-IDS2018

| 类别 | 数量 | 描述 |
| --- | --- | --- |
| Benign | 7373198 | 正常流 |
| BruteForce | 287597 | 一种旨在通过访问预定义可能性列表来获取用户名和密码凭据的技术 |
| Bot | 15683 | 一种攻击，使攻击者能够远程控制多台被劫持的计算机以执行恶意活动。 |
| DoS | 269361 | 试图使计算机系统的资源过载，目的是阻止对其数据的访问或可用性。 |
| DDoS | 380096 | 一种类似于 DoS 的尝试，但具有多个不同的分布式源。 |
| Infiltration | 62072 | 一种内部攻击，通过电子邮件发送恶意文件以利用应用程序，然后通过后门扫描网络以查找其他漏洞 |
| Web Attacks | 4394 | 包括 SQL 注入、命令注入和不受限制的文件上传的组 |

### 数据集特征维度

#### V1

| 特征 | 描述 |
| --- | --- |
| IPV4\_SRC\_ADDR | IPv4 源地址 |
| IPV4\_DST\_ADDR | IPv4 目标地址 |
| L4\_SRC\_PORT | IPv4 源端口号 |
| L4\_DST\_PORT | IPv4 目标端口号 |
| PROTOCOL | IP 协议标识符字节 |
| TCP\_FLAGS | 所有 TCP 标志的累积 |
| L7\_PROTO | 第 7 层协议（数字） |
| IN\_BYTES | 传入的字节数 |
| OUT\_BYTES | 传出字节数 |
| IN\_PKTS | 传入的数据包数 |
| OUT\_PKTS | 传出数据包数 |
| FLOW\_DURATION\_MILLISECONDS | 流持续时间（以毫秒为单位） |

#### V2

| 特征 | 描述 |
| --- | --- |
| IPV4\_SRC\_ADDR | IPv4 源地址 |
| IPV4\_DST\_ADDR | IPv4 目标地址 |
| L4\_SRC\_PORT | IPv4 源端口号 |
| L4\_DST\_PORT | IPv4 目标端口号 |
| PROTOCOL | IP 协议标识符字节 |
| L7\_PROTO | 应用程序协议（数字） |
| IN\_BYTES | 传入的字节数 |
| OUT\_BYTES | 传出字节数 |
| IN\_PKTS | 传入的数据包数 |
| OUT\_PKTS | 传出数据包数 |
| FLOW\_DURATION\_ MILLISECONDS | 流持续时间（以毫秒为单位） |
| TCP\_FLAGS | 所有 TCP 标志的累积 |
| CLIENT\_TCP\_FLAGS | 所有客户端 TCP 标志的累积 |
| SERVER\_TCP\_FLAGS | 所有服务器 TCP 标志的累积 |
| DURATION\_IN | 客户端到服务器流持续时间 （毫秒） |
| DURATION\_OUT | 客户端到服务器流持续时间 （毫秒） |
| MIN\_TTL | 最小流量 TTL |
| MAX\_TTL | 最大流量 TTL |
| LONGEST\_FLOW\_PKT | 流的最长数据包（字节） |
| SHORTEST\_FLOW\_PKT | 流的最短数据包（字节） |
| MIN\_IP\_PKT\_LEN | 观察到的最小流 IP 数据包的 Len |
| MAX\_IP\_PKT\_LEN | 观察到的最大流 IP 数据包的 Len |
| SRC\_TO\_DST\_SECOND\_ BYTES | Src 到 dst 字节/秒 |
| DST\_TO\_SRC\_SECOND\_ BYTES | Dst 到 src 字节/秒 |
| RETRANSMITTED\_IN\_ BYTES | 重新传输的 TCP 流字节数 （src->dst） |
| RETRANSMITTED\_IN\_ PKTS | 重新传输的 TCP 流数据包数 （src->dst） |
| RETRANSMITTED\_ OUT\_BYTES | 重新传输的 TCP 流字节数 （dst->src） |
| RETRANSMITTED\_ OUT\_PKTS | 重新传输的 TCP 流数据包数 （dst->src） |
| SRC\_TO\_DST\_AVG\_ THROUGHPUT | Src 到 dst 的平均 thpt （bps） |
| DST\_TO\_SRC\_AVG\_ THROUGHPUT | Dst 到 src 的平均 thpt （bps） |
| NUM\_PKTS\_UP\_TO\_ 128\_BYTES | IP 大小 <= 128 的数据包 |
| NUM\_PKTS\_128\_TO\_ 256\_BYTES | IP 大小> 128 且 <= 256 的数据包 |
| NUM\_PKTS\_256\_TO\_ 512\_BYTES | IP 大小> 256 且 <= 512 的数据包 |
| NUM\_PKTS\_512\_TO\_ 1024\_BYTES | IP 大小> 512 且 <= 1024 的数据包 |
| NUM\_PKTS\_1024\_TO\_ 1514\_BYTES | IP 大小> 1024 且 <= 1514 的数据包 |
| TCP\_WIN\_MAX\_IN | 最大 TCP 窗口 （src->dst） |
| TCP\_WIN\_MAX\_OUT | 最大 TCP 窗口 （dst->src） |
| ICMP\_TYPE | ICMP类型\*256+ICMP代码 |
| ICMP\_IPV4\_TYPE | ICMP类型 |
| DNS\_QUERY\_ID | DNS 查询事务 ID |
| DNS\_QUERY\_TYPE | DNS 查询类型（例如，1=A、2=NS..） |
| DNS\_TTL\_ANSWER | 第一个 A 记录的 TTL（如果有） |
| FTP\_COMMAND\_ RET\_CODE | FTP 客户端命令返回代码 |

## V1相关研究

### 二分类

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Models | Measurements | NF-BoT IoT | NF-ToN-IoT | NF-CSE CIC IDS2018 | NF-UNSW NB15 |  |
| Extra Trees ensemble classifier | Accuracy | 93.82% | 99.66% | 95.33% | 98.62% | [NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems | SpringerLink](https://link.springer.com/chapter/10.1007/978-3-030-72802-1_9) |
| Precision | 93.70% | 99.67% | 94.71% | 90.70% |
| Recall |  |  |  |  |
| F1-score | 97% | 100% | 83% | 85% |
| DIDS | Accuracy | 99.08% | 99.48% | 99.21% | 98.72% | [DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT - ScienceDirect](https://www.sciencedirect.com/science/article/pii/S277266222200073X#b50) |
| Precision | 99.03% | 99.48% | 99.21% | 98.69% |
| Recall | 99.08% | 99.48% | 99.21% | 98.72% |
| F1-score | 99.02% | 99.48% | 99.20% | 98.70% |
| CNN via transfer learning | Accuracy | 98.79% | 99.19% | 98.99% | 98.32% | [A Transfer Learning based Intrusion detection system for Internet of Things | Research Square](https://www.researchsquare.com/article/rs-2930837/v1) |
| Precision | 98.69% | 99.20% | 98.98% | 98.24% |
| Recall | 98.79% | 99.19% | 98.99% | 98.32% |
| F1-score | 98.67% | 99.19% | 98.98% | 98.26% |

### 多分类

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Models | Measurements | NF-BoT IoT | NF-ToN-IoT | NF-CSE CIC IDS2018 | NF-UNSW NB15 |  |
| Extra Trees ensemble classifier | Accuracy |  |  |  |  | [NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems | SpringerLink](https://link.springer.com/chapter/10.1007/978-3-030-72802-1_9) |
| Precision | 73.58% | 56.34 | 71.92 | 97.62 |
| Recall |  |  |  |  |
| F1-score | 77% | 60% | 80% | 98% |
| DIDS | Accuracy | 83.82% | 69.53% | 97.21% | 97.48% | [DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT - ScienceDirect](https://www.sciencedirect.com/science/article/pii/S277266222200073X#b50) |
| Precision | 78.64% | 56.84% | 96.35% | 97.11% |
| Recall | 83.82% | 69.53% | 97.21% | 97.48% |
| F1-score | 80.66% | 61.96% | 96.40% | 97.19% |
| KNN | Accuracy |  | 99% |  |  | [IoT Network Security: NetFlow Traffic Analysis and Attack Classification Using Machine Learning Techniques | IEEE Conference Publication | IEEE Xplore](https://ieeexplore.ieee.org/abstract/document/10522466) |
| Precision |  | 98.69% |  |  |
| Recall |  | 98.71% |  |  |
| F1-score |  | 98.7% |  |  |
| CNN via transfer learning | Accuracy | 83.67% | 70.54% | 97.53% | 97.21% | [A Transfer Learning based Intrusion detection system for Internet of Things | Research Square](https://www.researchsquare.com/article/rs-2930837/v1) |
| Precision | 87.13% | 59.91% | 96.62% | 96.59% |
| Recall | 83.67% | 70.54% | 97.53% | 97.21% |
| F1-score | 83% | 62% | 96% | 96% |