南京郵電大學
Nanjing University of Posts and Telecommunications

基于图神经网络的暗网流量检测方法及实现

汇报人：贾慰心

南京郵電大學
Nanjing University of Posts and Telecommunications

目录

CONTENTS

研究背景及意义

PART
01

02

03

04

暗网

人们通过传统搜索引擎访问到的只是互联网中的表层网络，仅是互联网这座冰山的一角。而隐藏在水下的、无法被传统搜索引擎访问的、更广阔的互联网区域，则被称为深网。而暗网是深网的一部分，必须借助特定的匿名通信工具才能访问，因其具有很强的匿名性，滋生了大量违法犯罪活动。暗网具有匿名性强、去中心化、路由动态性大等特性，使得其中的流量，即暗网流量总体呈现出隐蔽性强、非法性突出、追踪难度极大等特征。

法律法规

网络空间不是“法外之地”。网络空间是虚拟的，但运用网络空间的主体是现实的。近年来，网络安全法、数据安全法、个人信息保护法等重要法律法规相继推出，表明了国家层面对于网络空间安全的重视。

2021年王某因在暗网出售1.9亿条个人信息被判处2年并处罚金3万元。

2023年“净网行动”中，执法部门通过追踪加密通信日志，捣毁了一个涉案金额超过5亿元的暗网诈骗团伙。

研究内容与目标

01

PART
02

03

04

研究内容和目标

本课题：

基于图神经网络的暗网流量检测方法及实现

课题要求：

1. 了解暗网流量检测的背景理论；
2. 掌握使用Python、Sklearn、Pytorch等机器学习常用编程语言和工具库；
3. 实现一个暗网流量检测方法并在CIC-Darknet2020数据集上进行实验验证。

方法与实现

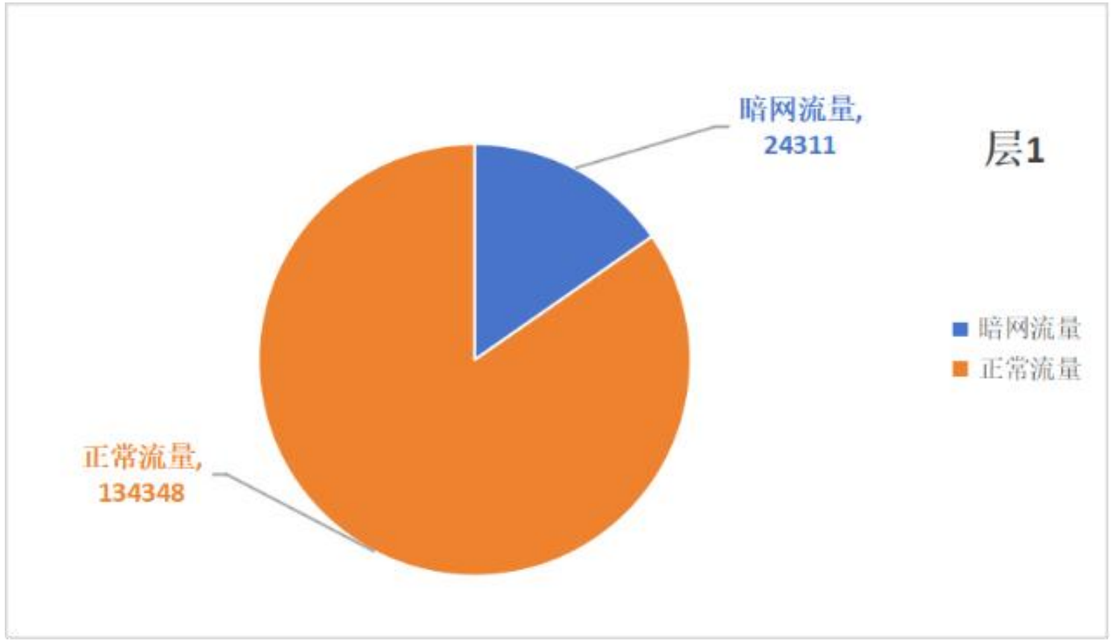
PART 03

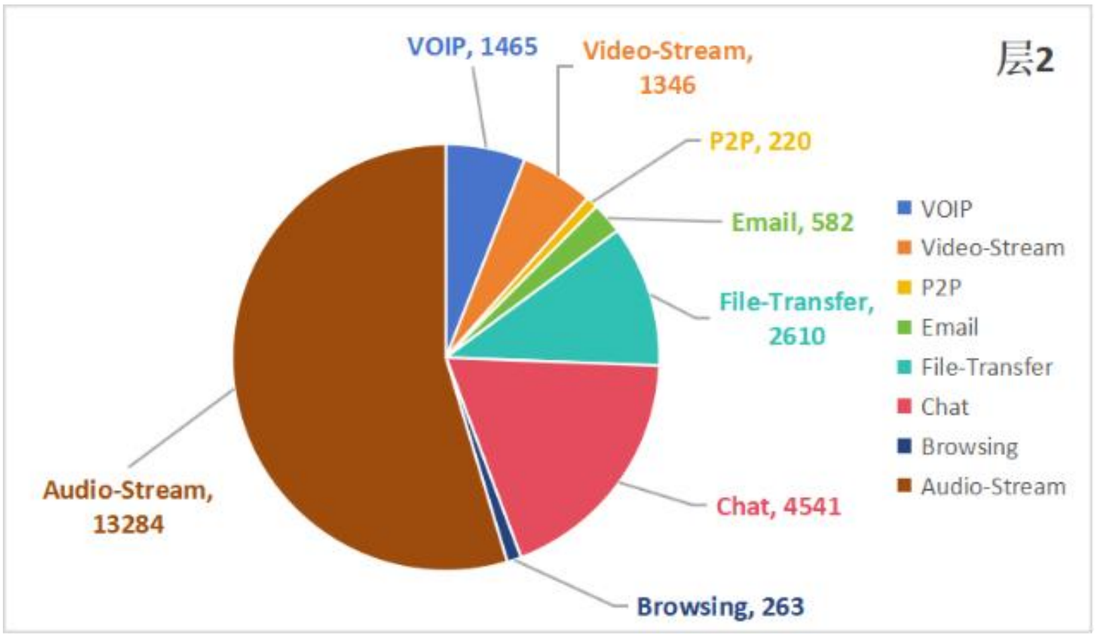
01 02 04

数据集

CIC-Darknet2020

本研究实验部分选用公开数据集CIC-Darknet2020来进行模型的训练与测试。该数据集是由新不伦瑞克大学加拿大网络安全研究所（CIC）于2020年发布的公开数据集，专门用于暗网流量检测和分析。该数据集整合了ISCXTor2016和ISCXVPN2016数据集，覆盖了更全面的暗网场景，共包含141530条样本和85个特征，且这些特征是对当前流量的统计特征。从标签结构上看，该数据集分为两层，第一层为正常流量和暗网流量；第二层为暗网流量类别的进一步细分，由特定应用程序生成，共涵盖八类常见应用场景。





数据预处理

数据清洗

对缺失值和异常值进行处理，原数据集中包含Nan值，对这些Nan值进行赋0，以解决可能出现的问题。然后删除无效特征列，如：时间戳、流ID，减少数据冗余。

地址映射

将源IP地址映射到172.16.0.1-172.31.0.1的地址区间。

一方面减少图结构内存占用；另一方面防止源节点为恶意流量提供无意标签，避免潜在的分类偏差。

标签编码

用数字来代替具体类别，方便进行分类评估。

数据保存

将处理好的数据保存，以便后续模型训练测试。

图结构构建

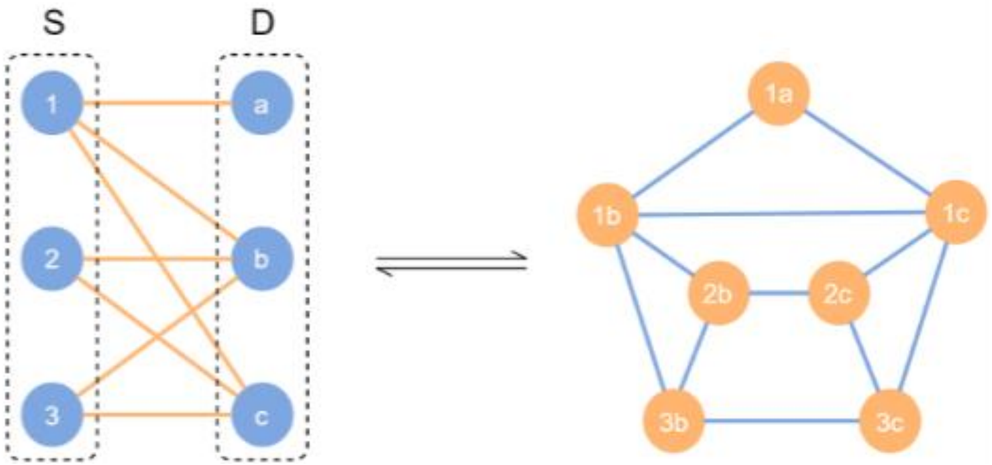
二分图G(S,D;E)的构建：

1.图的节点对应网络流量数据中的源地址和目的地址。

2.图的边对应流量记录。

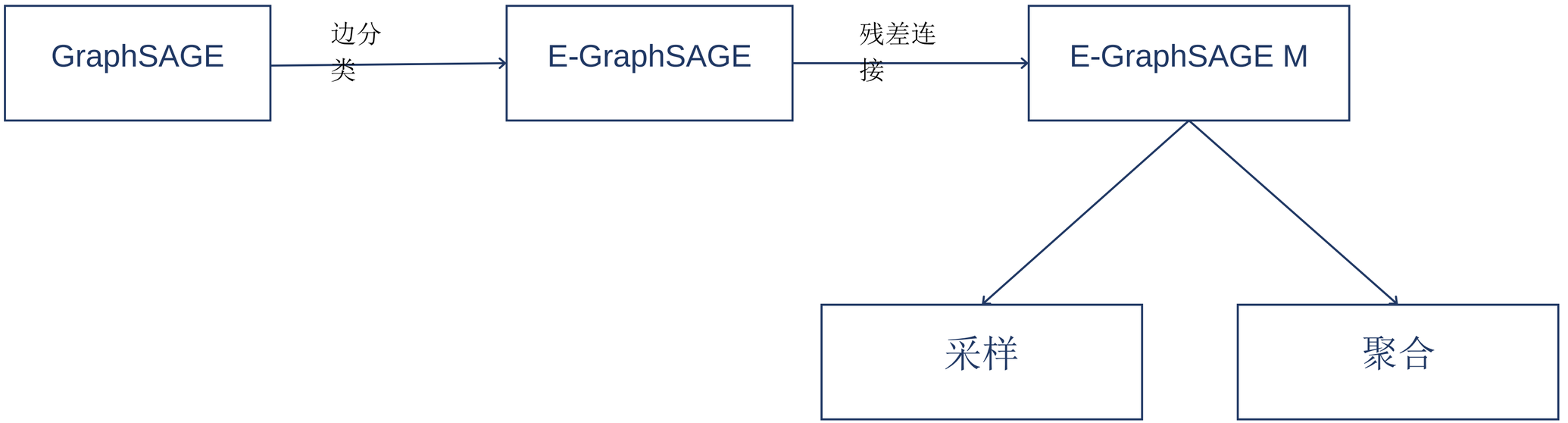
3.边特征对应流量的统计特征。

其中S、D、E分别表示源节点集、目的节点集、边集。暗网流量检测问题转化为图的边分类任务。



由于E-ResGAT算法是对节点进行分类的，为适应其特点，我们需要将二分图转换成线图。即：线图中的节点对应于原二分图的边，边则表示原二分图中共享同一个节点的两条边的连接关系。

E-GraphSAGE M模型



E-ResGAT模型

E-ResGAT算法的采样过程与E-GraphSAGE M算法类似，不过E-ResGAT使用的是线图中节点的全邻域。

E-ResGAT使用注意力机制来聚合邻域信息并在每一层都进行残差连接。

注意力机制对不同的邻居节点赋予不同的权重，从而更有效地聚合邻域信息。

残差连接：在每层聚合时，将原始特征与注意力机制聚合后的结果进行拼接，这样可以保留原始信息，避免在多层聚合过程中信息丢失，尤其是在处理高度不平衡的数据时，有助于防止少数类信息被多数类信息淹没。

实验设置

数据集的划分

测试集包含45000条样本，约占总体数据的30%，验证集包含5000条样本，约占总体数据的3%，其余数据为训练集。

通用设置

1.Pytorch深度学习框架

2.Adam优化器，学习率为0.03

3.交叉熵损失函数

4.训练过程采用分批次训练，每个批次大小设置为500；训练轮次为两个轮次。

基于E-GraphSAGE的模型实验设置：

1.模型层数K=2；

2.使用softmax作为分类器；

3.2跳8邻域采样；

4.聚合函数使用均值函数；

5.ReLU非线性激活函数。

基于GAT的模型实验设置：

1.模型层数K=3；

2.6头注意力机制；

3.使用softmax作为分类器；

4.全邻域采样；

5.ELU非线性激活函数。

实验结果评估（二分类）

表 3.1 基于图神经网络的暗网流量二分类评估结果

方法	评估指标				
	Accuracy	**Precision**	**Recall**	**F1**	**AUC**
E-GraphSAGE	0.9087	0.7280	0.6462	0.6846	0.9011
E-GraphSAGE M	0.9139	0.7444	0.6678	0.7040	0.9479
GAT	0.9168	0.7388	0.7072	0.7227	0.9452
E-ResGAT	**0.9220**	**0.7543**	**0.7285**	**0.7514**	**0.9553**

实验结果评估（多分类）

表 3.3 基于图神经网络的暗网多分类评估结果

方法	加权平均评估指标			宏观平均评估指标		
	Precision	**Recall**	**F1**	**Precision**	**Recall**	**F1**
E-GraphSAGE	0.8480	0.8817	0.8546	0.5166	0.3036	0.3240
E-GraphSAGE M	0.8641	0.8847	0.8613	**0.6104**	0.3860	0.3888
GAT	0.8598	0.8822	0.8645	0.4794	0.3003	0.3330
E-ResGAT	**0.8885**	**0.8867**	**0.8826**	0.5456	**0.4193**	**0.4335**

实验结果评估（多分类）

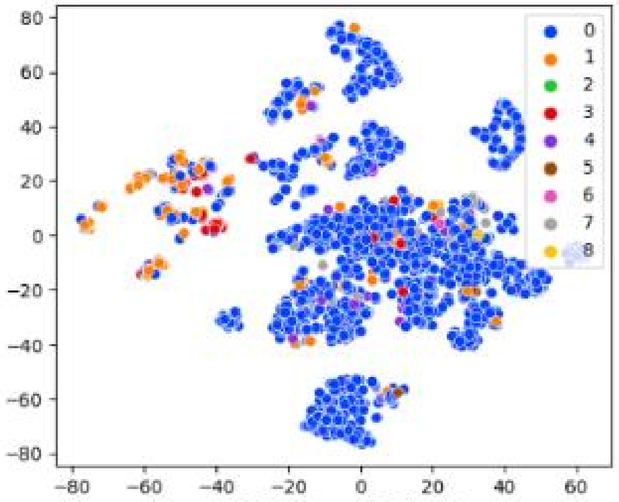
表 3.2 数据类别分布情况

类别	0	1	2	3	4	5	6	7	8
个数	42337	4188	83	1431	823	183	69	424	462

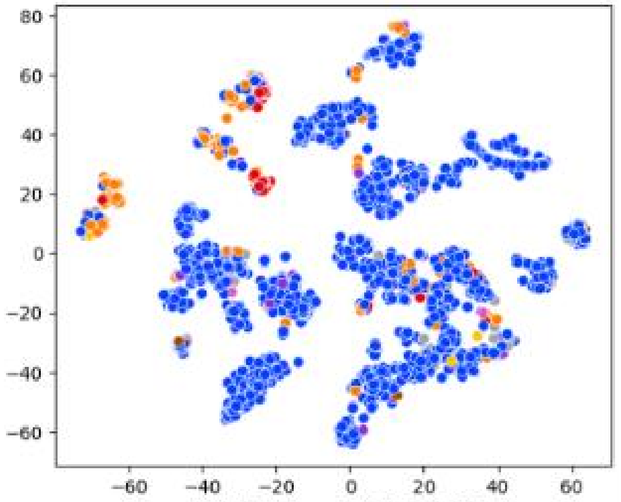
表 3.4 基于图神经网络多分类 F1 对比

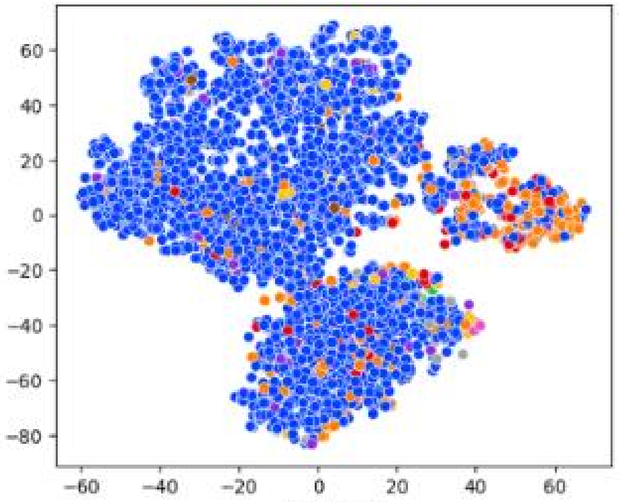
方法	各类 F1								
	0	1	2	3	4	5	6	7	8
E-GraphSAGE	0.9374	**0.6422**	0.3448	0.0081	0.0667	0	0.7819	0.0456	0.1909
E-GraphSAGE M	0.9449	0.6199	**0.5688**	0.0148	0.25	0	**0.7969**	0.1166	0.1875
GAT	0.9484	0.6122	0.3593	0.0892	**0.2951**	0.0103	0.5396	0.1882	0.1917
E-ResGAT	**0.9526**	0.6286	0.4600	**0.2396**	0.2880	**0.0909**	0.6838	**0.1912**	**0.1942**

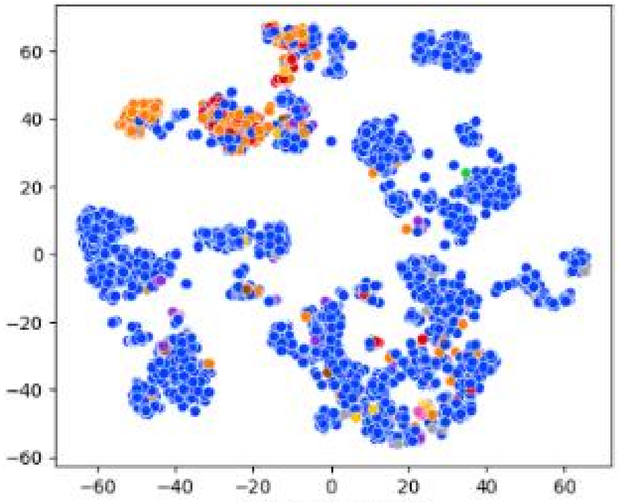
聚类效果可视化



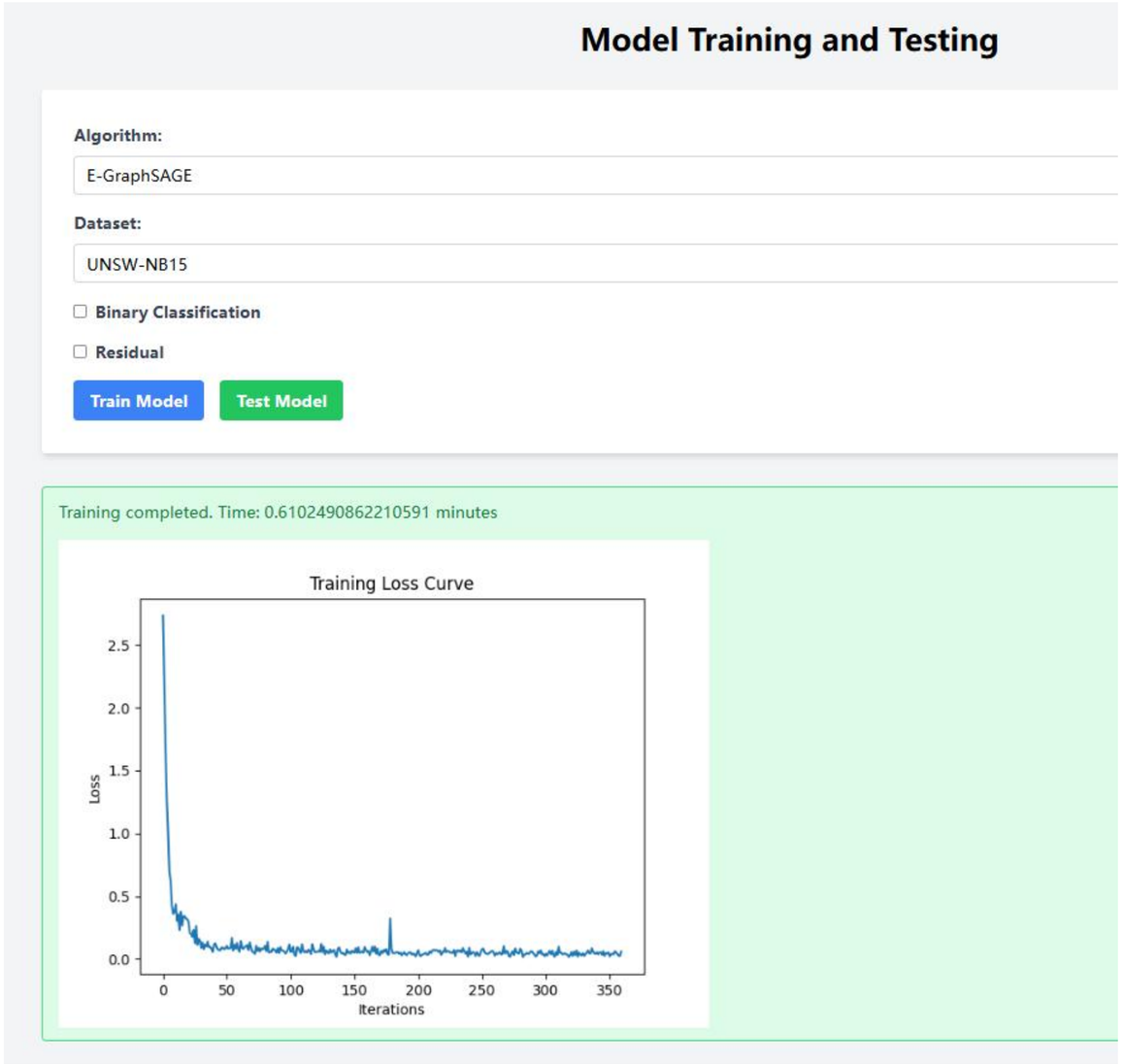
(a) E-GraphSAGE


(b) E-GraphSAGE M

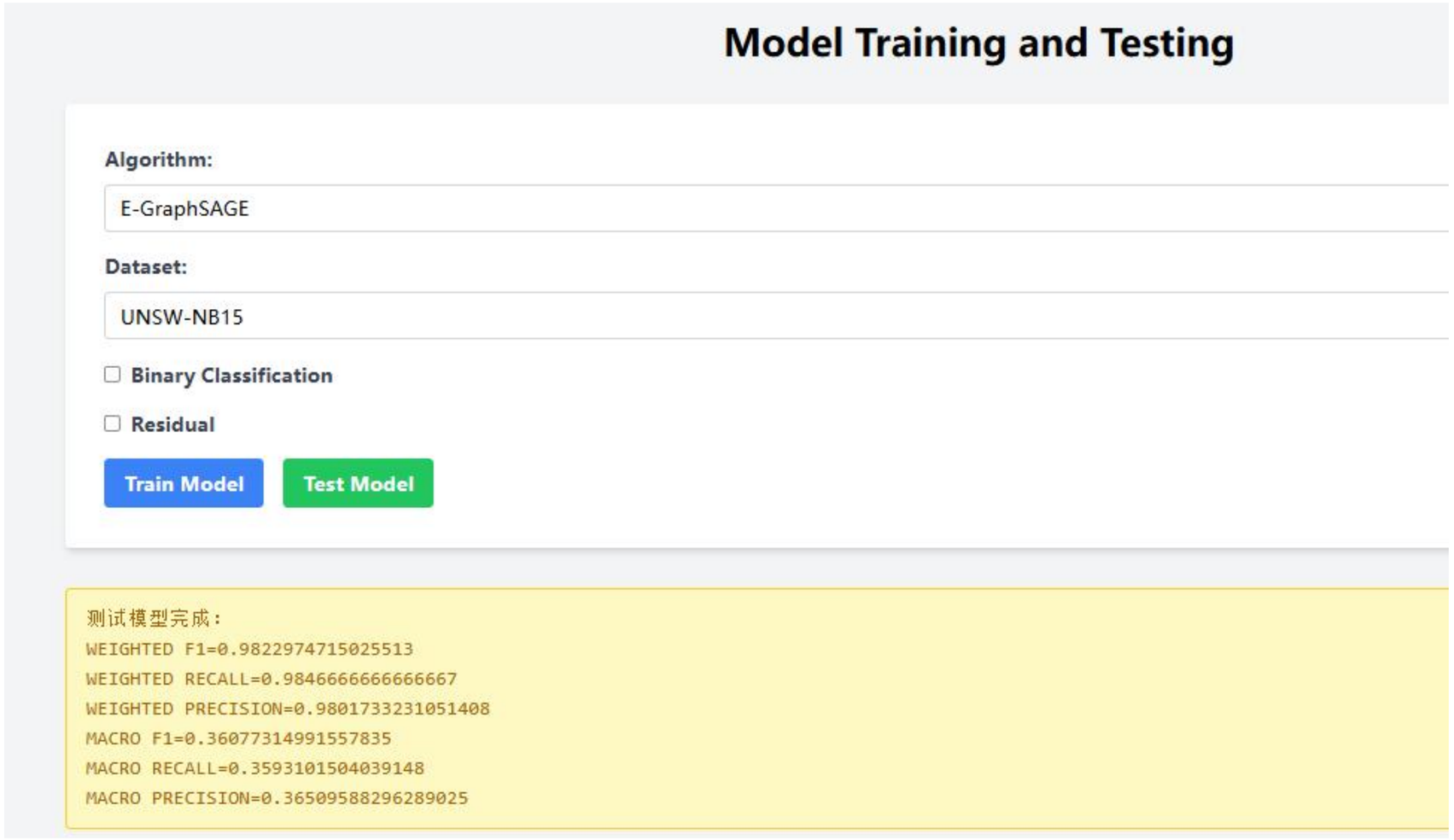

(c) GAT


(d) E-ResGAT

可视化界面展示（训练结果）



可视化界面展示（测试结果）



总结与展望

01 02 03

PART 04

总结与展望

总结

本课题针对暗网流量检测中动态路由混淆和极端类别不平衡两大挑战，基于现有图神经网络模型E-GraphSAGE和GAT，创新性地引入残差连接，实现了改进模型E-GraphSAGE M和E-ResGAT。在CIC-Darknet2020数据集上的实验结果表明，引入残差连接能够增强模型对暗网流量检测能力。

展望

1.优化图构建方法

2.结合数据增强算法

3.多源数据融合提高模型的泛化能力

感谢倾听

恳请各位老师批评指正