同行专家业内评价意见书编号：20240854191

附件1

浙江工程师学院（浙江大学工程师学院）
同行专家业内评价意见书

姓名： 宋卓学

学号： 22160274

申报工程师职称专业类别（领域）： 电子信息

浙江工程师学院（浙江大学工程师学院）制

2024年03月22日

一、个人申报

（一）基本情况【围绕《浙江工程师学院（浙江大学工程师学院）工程类专业学位研究生工程师职称评审参考指标》，结合该专业类别(领域)工程师职称评审相关标准，举例说明】

1.对本专业基础理论知识和专业技术知识掌握情况

申报人熟悉行业技术需求，系统掌握专业理论知识、专业技术知识和研究方法。在《基于深度学习的网络加密流量分析》项目中，申报人完成基于深度学习的网络加密流量分析方法综述调研，掌握此领域内基本知识，并产出专业报告《基于深度学习的网络加密流量分析方法综述》，对网络加密流量分析原理、业界典型公开或研究案例进行详实剖析。

申报人充分了解行业采用的新技术、新流程、新设备、先进生产方式、国内外技术前沿发展现状与趋势。在《基于深度学习的网络加密流量分析方法综述》专业报告中，申报人综述介绍网络加密流量分析方法的研究背景、现状及意义，对传统的网络流量分析方法包括基于端口匹配的网络流量分析、基于深度包检测的网络流量分析进行了回顾，并对现有基于机器学习和深度学习的加密流量分析文献方法进行了总结。申报人研究典型公开和研究案例，对基于深度学习的加密流量分析技术的一般性流程进行分析总结。此外，申报人总结了对网络加密流量分析方法进行评价的主要指标。在专业实践训练过程中，申报人不断积累情境性、意会性等知识，并逐步接触和了解多专业领域交叉知识。

综上，在基于深度学习的网络加密流量分析技术方面，申报人掌握当前主流的加密流量分析检测基本原理与国内外研究现状，掌握本专业基础理论知识和专业技术知识。

2.工程实践的经历

申报人承担企业应用性课题研究项目《基于深度学习的网络加密流量分析》。该项目针对网络流量这一网络活动的基本传输载体，对其进行识别和分类，重点研究基于深度学习的加密流量识别中的类增量学习与可解释性。
互联网的飞速发展和新一代信息技术的不断创新突破，已经给人们生活的方方面面带来了翻天覆地的变化。互联网逐渐成为生产生活的重要组成部分，使用人数也呈现出爆炸性的增长。网络流量是网络活动的基本传输载体，对网络流量进行识别和分类，对于提升网络服务质量、加强网络管理和保障网络安全显得尤为重要。

随着人们对隐私安全的重视，网络流量逐渐采用加密协议如SSL/TLS进行传输。虽然加密协议保护了用户的隐私，但它也给攻击者提供了躲避防火墙检测和网络监控的机会。例如，攻击者可以利用加密协议隐藏自己的入侵和攻击行为，通过加密流量隐匿明文特征。因此，加密流量给网络流量的识别与分类带来了新的挑战。随着近年来人工智能技术的发展，基于机器学习和深度学习的网络加密流量识别逐渐成为主流方法。

申报人在该项目中针对基于深度学习的加密流量识别中的类增量学习与可解释性展开研究，通过设计深度神经网络模型，实现可增量可解释的加密流量识别。具体地，该项目的主要研究内容包括:

(1)完成基于深度学习的加密流量分类方法综述调研。对基于深度学习的加密流量分类、业界典型公开或研究案例进行剖析，输出综述报告；
(2)可增量的加密流量识别。实际情形中网络应用或网络攻击的类型在不断产

生，现有的加密流量识别方法在该情形下往往需要重新训练整个模型以实现对新类别的识别，耗费大量的时间和存储空间。通过设计可增量的深度神经网络模型结构，使模型能够应对现实情形中的类增量场景。当新的类型出现时，不需要使用整个数据集重新训练整个模型，只需要使用新的数据轻量级地训练模型，就可以在保留旧类别分类能力的同时实现对新类别的识别；

(3)可解释的加密流量识别。由于深度学习的黑盒性，目前基于深度学习的加密流量识别方法缺乏可解释性，使用者无法获取识别结果的判断依据，也无法对流量类别的特征模式与类别间的相关程度形成直观认知。通过设计可解释的深度神经网络模型结构，使得模型的推理过程不再是完全黑盒，可以根据模型的计算过程，得到关于分类结果的判断依据、流量特征排名与类别间的距离画像；

(4)申报人在两个公开权威数据集CIC-IDS2017和ISCXVPN2016上评估了识别的效果、类增量学习的时间和空间开销以及模型可解释性的鲁棒性、稳定性和有效性，并给出了全局和局部的解释结果。

申报人承担整个项目研究的工作，完成全部研究内容，并提交相关综述报告，发表相应学术论文与发明专利。综述报告文档结构清晰，逻辑性强；代码可以实现研究内容中的各项功能，可读性强；学术论文是CCF-A类国际期刊水准，发明专利已获得授权。

3.在实际工作中综合运用所学知识解决复杂工程问题的案例（不少于1000字）

申报人具备技术应用创新及工程创新实践能力，能够综合运用所学知识解决复杂工程问题，对本领域工作进行设计、过程审核和设计质量把关，有效规避设计质量问题，通过技术应用创新、成果转化、解决企业工程实际问题等，取得良好的经济和社会效益。申报人掌握参与工程建设所需的基本技能，能综合运用先进仪器设备、专业软件、企业现场数据采集与算法分析等现代研究工具和研究方法开展工程建设和项目研究工作，综合养成工程思维。

(1)在《基于深度学习的网络加密流量分析》这一项目中，申报人首先设计了指纹学习LSTM，用于捕获不同流量类型的指纹。所谓指纹学习过程是使得当前状态的输出和下一个时间步的输入之间尽可能接近。在分类阶段，计算每个时间步上状态的输出和下一个时间步输入之间的损失，预测结果由损失最小的指纹 LSTM确定；

(2)在设计了指纹学习过程的基础上，申报人基于指纹学习LSTM构建可增量模型。模型维护了一个指纹列表，指纹列表中有多个指纹模块，每个指纹模块都有一组与流量类型相对应的独立参数。如果模型要具备识别新流量类型的能力，唯一需要做的就是在指纹列表中引入一个新的指纹模块，并用新的流量数据训练这个模块。这使得模型具有对新流量类型进行类增量学习的能力，而无需重新训练现有的指纹模块。此外，申报人在类增量更新时的损失函数中加入类间区分度损失和稀疏参数损失，使新增指纹单元与现有指纹单元间有更好的区分度，并减少模型参数的存储空间；

(3)申报人基于指纹学习LSTM构建模型的可解释性。该方法从指纹学习过程中指纹损失的计算和比较过程切入，量化分析每一维特征对识别结果的贡献度，从而得到特征的重要性排名、识别结果的特征归因以及流量类别间的相似距离画像，对流量识别模型进行全局和局部的解释。相比于现有的可解释方法，该方法考虑了流量指纹特征的时序关系；

(4)申报人在两个公开权威数据集上评估了识别的效果、类增量学习的时间和空间开销以及模型可解释性的鲁棒性、稳定性和有效性，并给出了全局和局部的解释结果。评估结果显示

，项目提出的方法具有优于现有SOTA方法的加密流量识别效果，并且在类增量场景下具有更低的时间和空间开销。此外，相比于现有的可解释方法，项目提出的模型可解释方法具有更强的鲁棒性、稳定性和有效性；

(5)申报人承担整个项目的研究工作，完成了全部研究内容，项目整体交付满足功能要求的可运行代码，核心算法模型发表了CCF-A类国际期刊论文，获得发明专利授权；

(6)申报人具备良好的团队协作能力与交流、竞争、合作的能力，项目实践过程中每双周提交进度报告，每月底进行研究进展汇报与问题讨论。此外，申报人定期系统地分析CCF-A类国际会议与期刊论文中网络加密流量分析相关技术与发展趋势，输出综述报告并交流分享；

(7)申报人具有良好的环境及岗位适应能力，全过程参与企业实际工程项目建设，能应对压力和挑战，加强自身对环境和岗位的适应力，具备从事工程技术研究、设计、生产、技术管理决策实战经验。

（二）取得的业绩（代表作）【限填3项，须提交证明原件（包括发表的论文、出版的著作、专利证书、获奖证书、科技项目立项文件或合同、企业证明等）供核实，并提供复印件一份】

1.
公开成果代表作【论文发表、专利成果、软件著作权、标准规范与行业工法制定、著作编写、科技成果获奖、学位论文等】

成果名称	成果类别 [含论文、授权专利（含发明专利申请）、软件著作权、标准、工法、著作、获奖、学位论文等]	发表时间/授权或申请时间等	刊物名称/专利授权或申请号等	本人排名/总人数	备注
I2RNN: An Incremental and Interpretable Recurrent Neural Network for Encrypted Traffic Classification	国际期刊	2023年02月28日	IEEE Transactions on Dependable and Secure Computing	1/7	
一种基于深度学习的网络流量过滤规则转化方法	授权发明专利	2021年12月10日	专利号：ZL202111043954.7	2/5	

2.其他代表作【主持或参与的课题研究项目、科技成果应用转化推广、企业技术难题解决方案、自主研发设计的产品或样机、技术报告、设计图纸、软课题研究报告、可行性研究报告、规划设计方案、施工或调试报告、工程实验、技术培训教材、推动行业发展中发挥的作用及取得的经济社会效益等】

（三）在校期间课程、专业实践训练及学位论文相关情况	
课程成绩情况	按课程学分核算的平均成绩： 87 分
专业实践训练时间及考核情况(具有三年及以上工作经历的不作要求)	累计时间： 1 年（要求1年及以上） 考核成绩： 90 分（要求80分及以上）
本人承诺	
个人声明：本人上述所填资料均为真实有效，如有虚假，愿承担一切责任，特此声明！ **申报人签名：** 宋卓学	

22160274

二、日常表现考核评价及申报材料审核公示结果

日常表现考核评价	非定向生由德育导师考核评价、定向生由所在工作单位考核评价： ☑优秀 ☐良好 ☐合格 ☐不合格 德育导师/定向生所在工作单位分管领导签字（公章）：朱辰 2022年3月25日
申报材料审核公示	根据评审条件，工程师学院已对申报人员进行材料审核（学位课程成绩、专业实践训练时间及考核、学位论文、代表作等情况），并将符合要求的申报材料在学院网站公示不少于5个工作日，具体公示结果如下： ☐通过 ☐不通过（具体原因： ） 工程师学院教学管理办**公室**审核签字（公章）： 年 月 日

浙 江 大 学 研 究 生 院

攻读硕士学位研究生成绩表

学号：22160274	姓名：宋卓学	性别：男	学院：工程师学院	专业：计算机技术	学制：2.5年
毕业时最低应获：24.0学分	已获得：25.0学分			入学年月：2021-09	毕业年月：2024-03
学位证书号：1033532024602228			毕业证书号：103351202402600454		授予学位：电子信息硕士

学习时间	课程名称	备注	学分	成绩	课程性质	学习时间	课程名称	备注	学分	成绩	课程性质
2021-2022学年秋季学期	GPU计算与工程应用		2.0	80	专业选修课	2021-2022学年夏季学期	研究生英语		2.0	免修	公共学位课
2021-2022学年秋冬季学期	中国特色社会主义理论与实践研究		2.0	88	公共学位课	2021-2022学年夏季学期	自然辩证法概论		1.0	77	公共学位课
2021-2022学年秋冬季学期	数据分析的概率统计基础		3.0	92	专业选修课	2021-2022学年夏季学期	物联网信息安全技术与应用基础		2.0	99	专业学位课
2021-2022学年秋冬季学期	研究生论文写作指导		1.0	93	专业学位课	2021-2022学年夏季学期	大数据与人工智能工程应用		2.0	93	专业学位课
2021-2022学年秋冬季学期	电子与信息工程技术管理		2.0	92	专业学位课	2021-2022学年夏季学期	移动互联网智能设备应用设计与实践		3.0	85	专业学位课
2021-2022学年冬季学期	物联网操作系统与边缘计算		2.0	93	专业选修课	2021-2022学年春夏季学期	工程伦理		2.0	95	公共学位课
2021-2022学年夏季学期	研究生英语基础技能		1.0	免修	公共学位课						

说明：1.研究生课程按三种方法计分：百分制，两级制（通过、不通过），五级制（优、良、中、及格、不及格）。

2.备注中“*”表示重修课程。

学院成绩校核章：

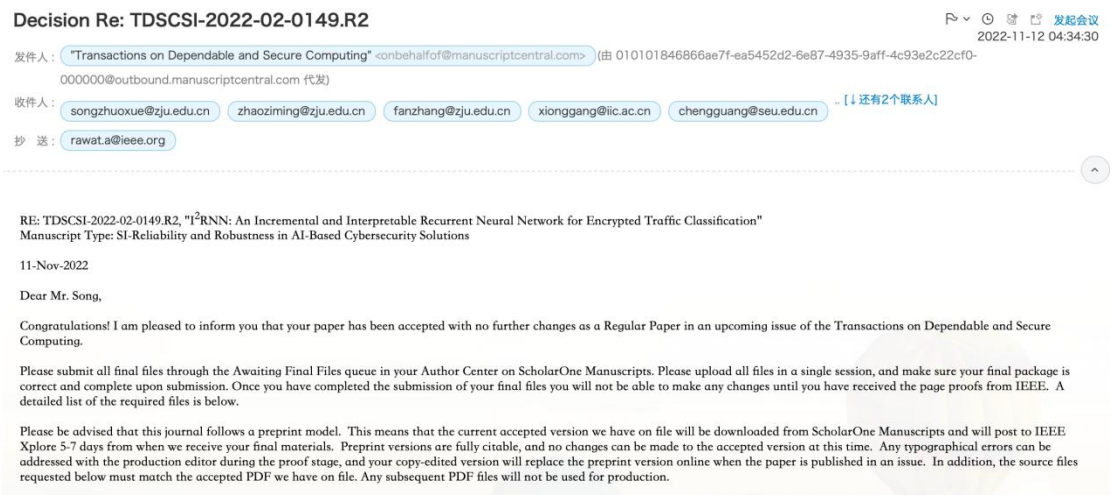
成绩校核人：张梦依

打印日期：2024-04-02

论文成果（已录用，排名 1/7）

I^2RNN: An Incremental and Interpretable Recurrent Neural Network for Encrypted Traffic Classification, IEEE Transactions on Dependable and Secure Computing (IEEE TDSC, CCF-A)

接收邮件：



Decision Re: TDSCSI-2022-02-0149.R2

2022-11-12 04:34:30

发件人："Transactions on Dependable and Secure Computing" <onbehalfof@manuscriptcentral.com> (由 010101846866ae7f-ea5452d2-6e87-4935-9aff-4c93e2c22cf0-000000@outbound.manuscriptcentral.com 代发)

收件人：songzhuoxue@zju.edu.cn zhaoziming@zju.edu.cn fanzhang@zju.edu.cn xionggang@iic.ac.cn chengguang@seu.edu.cn [↓还有2个联系人]

抄 送：rawat.a@ieee.org

RE: TDSCSI-2022-02-0149.R2, "I^{2}RNN: An Incremental and Interpretable Recurrent Neural Network for Encrypted Traffic Classification"
Manuscript Type: SI-Reliability and Robustness in AI-Based Cybersecurity Solutions

11-Nov-2022

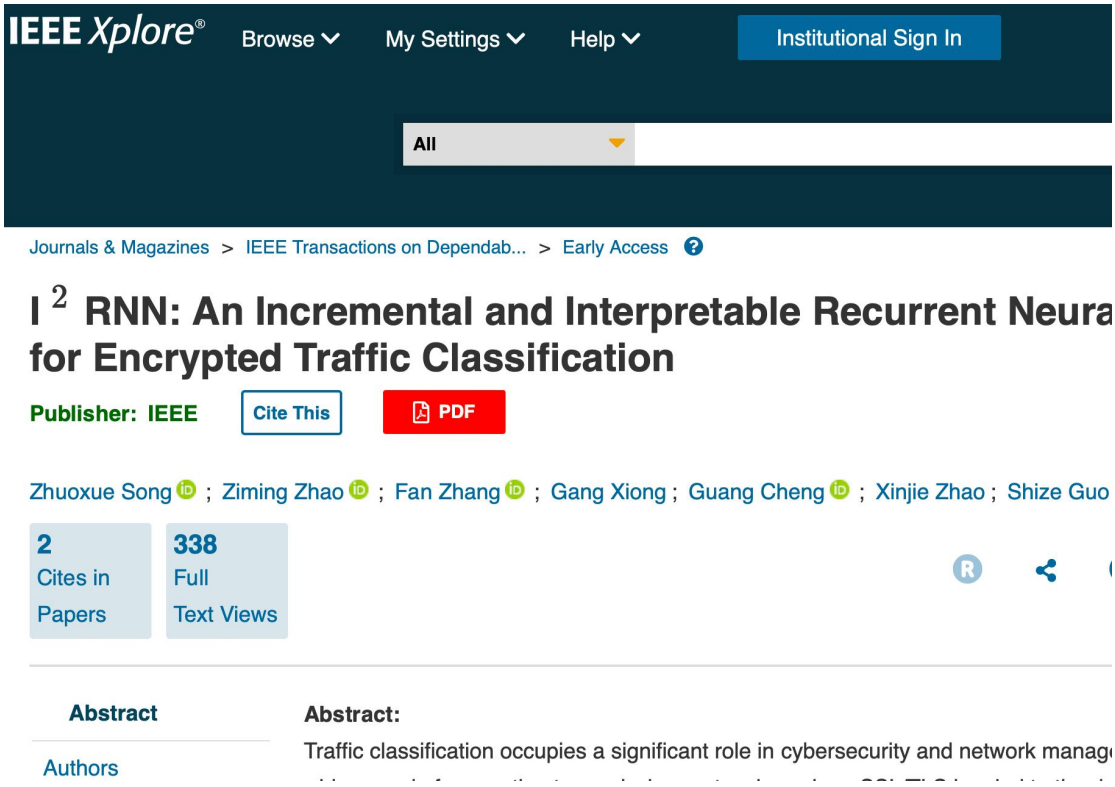
Dear Mr. Song,

Congratulations! I am pleased to inform you that your paper has been accepted with no further changes as a Regular Paper in an upcoming issue of the Transactions on Dependable and Secure Computing.

Please submit all final files through the Awaiting Final Files queue in your Author Center on ScholarOne Manuscripts. Please upload all files in a single session, and make sure your final package is correct and complete upon submission. Once you have completed the submission of your final files you will not be able to make any changes until you have received the page proofs from IEEE. A detailed list of the required files is below.

Please be advised that this journal follows a preprint model. This means that the current accepted version we have on file will be downloaded from ScholarOne Manuscripts and will post to IEEE Xplore 5-7 days from when we receive your final materials. Preprint versions are fully citable, and no changes can be made to the accepted version at this time. Any typographical errors can be addressed with the production editor during the proof stage, and your copy-edited version will replace the preprint version online when the paper is published in an issue. In addition, the source files requested below must match the accepted PDF we have on file. Any subsequent PDF files will not be used for production.

IEEE Xplore 数据库搜索：



IEEE Xplore® Browse My Settings Help Institutional Sign In

All

Journals & Magazines > IEEE Transactions on Dependab... > Early Access

I ^{2} RNN: An Incremental and Interpretable Recurrent Neura for Encrypted Traffic Classification

Publisher: IEEE Cite This PDF

Zhuoxue Song ; Ziming Zhao ; Fan Zhang ; Gang Xiong ; Guang Cheng ; Xinjie Zhao ; Shize Guo

2 Cites in Papers

338 Full Text Views

Abstract

Authors

Abstract:

Traffic classification occupies a significant role in cybersecurity and network manag

论文原文链接：https://ieeexplore.ieee.org/document/10056861

I^2RNN: An Incremental and Interpretable Recurrent Neural Network for Encrypted Traffic Classification

Zhuoxue Song, Ziming Zhao, Fan Zhang, *Member, IEEE*, Gang Xiong, Guang Cheng, *Member, IEEE*, Xinjie Zhao, and Shize Guo

***Abstract*—Traffic classification occupies a significant role in cybersecurity and network management. The widespread of encryption transmission protocols such as SSL/TLS has led to the dominance of deep learning based approaches. In cybersecurity, strong adversaries often complicate their strategies by constantly developing emerging attacks. Meanwhile, security practitioners desire to grasp the reasons for inference results. However, existing deep learning approaches lack efficient adaptation for incremental traffic types and often have less interpretability. In this paper, we propose I^2RNN, an Incremental and Interpretable Recurrent Neural Network for encrypted traffic classification. The I^2RNN proposes a novel propagation process to extract the sequence fingerprints from sessions with local robustness. Meanwhile, this proposal provides interpretability including time-series feature attribution and inter-class similarity portrait. Moreover, we design I^2RNN in an incremental manner to adapt to emerging traffic types. The I^2RNN only needs to train an additional set of parameters for the newly added traffic type rather than retraining the whole model with the entire dataset. Extensive experimental results show that our I^2RNN can achieve remarkable performance in traffic classification, incremental learning, and model interpretability. Compared with other local interpretability methods, our I^2RNN exhibits excellent stability, robustness, and effectiveness in the interpretation of network traffic data.**

***Index Terms*—Encrypted traffic classification, incremental learning, interpretability, recurrent neural network.**

Manuscript received 17 February 2022; revised 10 November 2022; accepted 11 November 2022. This work was supported in part by the National Natural Science Foundation of China under Grants 62227805 and 62072398, in part by SUTD-ZJU IDEA for visiting professors under Grant SUTD-ZJUVP201901, in part by the National Key R&D Program of China under Grant 2020AAA0107700, in part by the Alibaba-Zhejiang University Joint Institute of Frontier Technologies, in part by Zhejiang Key R&D Plan under Grant 2021C01116, in part by the Leading Innovative and Entrepreneur Team Introduction Program of Zhejiang under Grant 2018R01005, in part by the Research Institute of Cyberspace Governance in Zhejiang University, in part by the National Key Laboratory of Science and Technology on Information System Security under Grant 6142111210301, in part by the State Key Laboratory of Mathematical Engineering and Advanced Computing, and in part by the Key Laboratory of Cyberspace Situation Awareness of Henan Province under Grant HNTS2022001. *(Corresponding author: Fan Zhang.)*

Zhuoxue Song, Ziming Zhao, Xinjie Zhao, and Shize Guo are with the College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China (e-mail: songzhuoxue@zju.edu.cn; zhaoziming@zju.edu.cn; zhaoxinjieem@163.com; nsfgsz@126.com).

Fan Zhang is with the College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China, and with the ZJU-Hangzhou Global Scientific and Technological Innovation Center, Hangzhou 311200, China, and with the Key Laboratory of Blockchain and Cyberspace Governance of Zhejiang Province, Jiaxing Research Institute, Zhejiang University, Jiaxing 314000, China, and also with the Zhengzhou Xinda Institute of Advanced Technology, Zhengzhou 450001, China (e-mail: fanzhang@zju.edu.cn).

Gang Xiong is with the Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100190, China (e-mail: xionggang@iie.ac.cn).

Guang Cheng is with the School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China (e-mail: chengguang@seu.edu.cn).

Digital Object Identifier 10.1109/TDSC.2023.3245411

I. Introduction

TRAFFIC classification is important to the entire network for many different purposes, such as network management, Quality of Service (QoS) guarantees, and cybersecurity [1], [2], [3]. Over the last decades, the volume of traffic starts to be encrypted by application-layer encryption transmission protocols, such as Secure Socket Layer/Transport Layer Security (SSL/TLS) [4], [5]. Such encryption technology protects the privacy of Internet users, yet it provides attackers chances to evade firewall detection and circumvent surveillance systems. For example, an attacker may exploit encryption technology to invade and attack the system anonymously. That is to say, encryption technology brings new challenges to traffic identification. Therefore, the classification of encrypted traffic has attracted great attention in both academia and industry [6].

Previous traffic classification methods can be roughly divided into four main categories: port-based [7], payload-based [8], [9], machine-learning-based (ML-based) [10], [11], and deep-learning-based (DL-based) [12], [13]. The wide adoption of traffic encryption techniques, such as the SSL/TLS protocols, causes traditional port-based and payload-based methods to nearly fail. The payload values in packets can be considered as totally *randomized* after cryptographic encryption [14], which are extremely difficult (nearly impossible to some extent) for those port-based and payload-based methods to handle. Therefore, many researchers turn to ML-based and DL-based methods, which have become the mainstream methods for encrypted traffic classification nowadays.

The workflow of traffic classification with machine learning mainly contains two phases, namely feature engineering and model training [15]. The former is to design and select statistical features from traffic flows, such as the average packet length, the average interval of packet arrival time, the maximum TCP window size, etc. The latter is to feed the features into a specific classification model, e.g., SVM [16]. Both phases will directly affect the eventual performance and effectiveness of the classification. Meanwhile, the ML-based method is especially dependent on the so-called feature selection process which requires the sophisticated experience of those experts in the area. Therefore, many *end-to-end* or nearly *end-to-end* methods based on deep learning were proposed as in demand [17], [18]. These

证书号第4840496号

发明专利证书

发明名称：一种基于深度学习的网络流量过滤规则转化方法

发明人：张帆;宋卓学;赵子鸣;陈欢;李亮

专利号：ZL 2021 1 1043954.7

专利申请日：2021年09月07日

专利权人：浙江大学

地址：310058 浙江省杭州市余杭塘路866号

授权公告日：2021年12月10日　　授权公告号：CN 113489751 B

国家知识产权局依照中华人民共和国专利法进行审查，决定授予专利权，颁发发明专利证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。专利权期限为二十年，自申请日起算。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

局长
申长雨

国家知识产权局

2021年12月10日

其他事项参见续页

证书号第4840496号

国家税务总局北京市海淀区税务局 印花税 代扣专用章 国家知识产权局

专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年09月07日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

申请日时本专利记载的申请人、发明人信息如下：

申请人：

浙江大学

发明人：

张帆；宋卓学；赵子鸣；陈欢；李亮