




Received March 6, 2021, accepted March 19, 2021, publication date of March 23, 2021, 当前版本日期 2021年4月9日。

数字对象标识符 10.1109/ACCESS.2021.3068267

# 基于进化算法和网络 启用架构搜索的多目标 流量分类

XIAOJUAN WANG , XINLEI WANG , LEI JIN , RENJIAN LV<sup>1,2</sup>, BINGYING DAI<sup>3</sup>,

MINGSHU HE<sup>1</sup>, AND田七吕

<sup>1</sup>北京邮电大学电子工程学院,北京 100876

<sup>2</sup>华北计算技术研究所,北京 100083

<sup>3</sup>科罗拉多州立大学统计系,柯林斯堡,CO 80523,美国

通讯作者: 雷进 (jinlei@bupt.edu.cn)

这项工作得到了中国国家自然科学基金资助,资助号为 61871046。

**摘要**网络流量分类技术在网络安全管理中发挥着重要作用。然而,传统方法的固有局限性越来越明显,无法解决现有的流量分类任务。最近,神经架构搜索 (NAS) 作为一种自动化手动架构构建过程的工具引起了广泛关注。为此,本文提出基于多目标进化算法 (MOEAs)的NAS对恶意网络流量进行分类。主要目的是通过降低模型的空间比例和通道数来简化搜索空间。此外,在有效搜索空间改变搜索策略,采用的策略包括带有精英保留策略的非支配排序遗传算法 (NSGA-II)、强度帕累托进化算法 (SPEA-II)和多目标粒子群算法优化 (MOPSO)来解决制定的多目标NAS。通过对种群收敛次数、模型精度、Pareto最优集、模型复杂度和策略运行速度的综合比较,得出基于NSGA-II搜索的模型性能最好。

比较了当前机器学习算法和基于网络的人工学习方法的实验结果,表明我们的方法在两个公共数据集上取得了更好的分类性能,计算复杂度较低,主要由 FLOPs 衡量。我们的方法能够在 IDS2012 和 ISCX VPN 数据集上分别以 11.501 MB 和 4.718 MB 的 FLOP 实现 99.806% 和 99.369% 的 F1 分数。

**INDEX TERMS**深度学习、多目标、神经结构搜索、流量分类。

## 1. 引言网络流量分类

是一项基本任务,可用于检测网络入侵或提供适当的网络服务。最近,由于多种原因,流量分类变得越来越具有挑战性。一是网络应用多样化,网络流量种类大幅增加。其次,越来越多的网络应用程序使用加密协议。深度包检测 (DPI) 等经典方法无法解析加密流量。

第三,实时流量分类需要一个模型

副主编协调审阅这份手稿和  
批准出版的是潘肇庆



更低的复杂度和更好的运行速度来保证分类性能。

基于端口的方法 [1] 和 DPI [2] 在处理加密场景时无效。为了解决这个棘手的问题,提出了基于特征的方法 [3]。在人工提取网络流量的相关特征后,研究人员使用支持向量机 (SVM)[4]、[5]和随机森林 (RF)[6]、[7]等机器学习 (ML)算法来拟合交通数据。然而,从网络流量中提取特征需要相关的专业知识,并且可能会导致信息丢失。深度学习 (DL) 适用于将原始数据直接发送到基于 DL 的模型中。先前的研究 [8]-[10] 提出了设计良好的卷积神经网络 (CNN) 用于分类

交通流量问题。AutoML [11]、[12] 的兴起启发了我们自动构建可应用于流量分类任务的网络。AutoML 的优势是显而易见的。首先,它可以提高模型性能。此外,网络架构设计中的人为干预也将大大减少。

在之前的研究中,只使用了简单的一维和二维卷积层或全连接层。最近,一些有用的卷积块,例如 ResNet [13] 中使用的 bottleneck 和分割任务中使用的扩张卷积 [14]、[15],提高了计算机视觉领域的网络性能。确定如何将这有用的网络块应用于流量分类任务仍然是一个棘手的问题。因此,研究人员倾向于使用 AutoML [34]、[35] 来处理它。适用于我们场景的神经架构搜索 (NAS)是AutoML的一个重要分支。NAS 寻求自动化网络架构设计过程。一些工作[16]、[17]一般将NAS视为单目标优化问题,只关注提高分类效果而忽略了结构的高复杂性。然而,一些网络攻击(例如,DDoS)逐渐集中在移动端[57],因此当DL训练模型在资源受限的移动设备上实现时,需要考虑模型是否满足被访问的要求。从多个角度看轻量化[36]。因此,为了平衡模型的分类精度和复杂度,我们使用多目标优化算法(MOAs),包括具有精英策略的非支配排序算法(NSGA-II)、强度帕累托进化算法(SPEA-II)和多目标粒子群优化(MOPSO),完成搜索。然后再次从网络参数个数、FLOPs、MAccs(乘法累加运算)等方面对模型的轻量级性能进行评估,以评估上述MOAs的有效性。此外,我们在NAS架构的搜索空间中添加了更多预定义的操作块结构,以获得更高的性能。我们在两个通用网络流量数据集上测试搜索模型,以验证设计搜索空间的效率。

以下是我们的主要工作: 我们定义了五个块和流行的操作来简化搜索空间。在消融实验中,我们证明可以搜索具有较低空间比和通道数量的块来寻找具有较低计算复杂性和较高 F1 分数的模型。然后,基于选定的搜索空间,使用三种多目标搜索策略来确定同一数据集上总体的 Pareto 边界。最后,我们从 Pareto 边界中选择理想的架构,并比较它们的 F1 分数、复杂性、轻量级和速度。

一般来说,最佳搜索策略是根据整体搜索情况和搜索到的最优架构来确定的。

本文的创新点如下:

- (1) **简化搜索空间**:我们提出了一个改进的搜索空间,主要包括改变

基于NSGA-II的NAS的通道和空间比例(主要是为了获得最优搜索空间)。消融研究显示了这些改进的效率。

- (2) **优化搜索策略**:我们使用基于进化算法(EAs)的不同架构搜索策略来自动生成近似帕累托集(PS)的CNN架构种群,与现有的相比,它可以实现低复杂度和高权重的F1-score手工制作的神经网络作品。

- (3) **评估开发模型的性能**:在比较性能和模型复杂性后,选择基于三种优化算法的帕累托最优(PO)。从不同方面分析了最优模型的轻量化部署。

本文的其余部分安排如下。第二节介绍了本文的相关工作。第三节显示了搜索块结构和搜索策略的详细信息。

第四节验证了我们搜索架构的有效性。第五节给出了结论。

## 二.相关工作

考虑到本文提出的模型旨在清楚地展示基于 MOEA 任务的恶意流量分类,文献综述分为三个部分。

第一部分介绍流量分类和该领域专家以前的工作。第二部分回顾了NAS及其重要方法的介绍。在第三部分,我们重新整理了包括早期经典和最先进的 MOEAs 在内的相关算法,并分析了 NSGA-II、SPEA-II 和 MOPSO 算法的应用,主要侧重于便利性和高可行性它在现实世界问题中的应用所带来的。

### A. 流量分类

目前主要有两种流量分类方法:一种是基于ML,另一种是基于神经网络。

Al-Obaidy等人。[17]系统地评估了四种监督 ML 方法的社交媒体流量分类性能,即 SVM、朴素贝叶斯、C4.5 和 MLP。作者提取了 14 个基于流的特征,包括源 IP 地址和目标 IP 地址。随着特征数量的不断增加,流量分类结果也逐渐提高。事实证明,C4.5生成的规则在基于流特征的数据集上表现最好,准确率最高,达到86.33%。考虑到智能系统(拖拉机)的设计以改进对恶意流量的分析,Muliukha等人。[18]主要使用 RF 和朴素贝叶斯分类器分别对 VPN 连接和 SSL 流量进行分类。结果表明,RF的平均分类准确率为87.9% (±0.60%);然而,使用朴素贝叶斯分类器对不同类型的流量进行分类时,准确率差异较大,最高准确率达到99.1379%,最低准确率仅为33.33%。ML 的分类精度在很大程度上取决于特征工程,这需要

大量的手工工作。人工提取的特征是浅层特征,更多的全局特征和局部特征可以提高评估的准确性[58]。

DL 可以通过每一层自动选择特征 [59]。DL 的学习能力远高于 ML,可以学习到复杂度更高的模型。

CNN模型在[19]中设计用于检测恶意URL,从而节省了特征提取的步骤。为了解决端到端的加密流量分类,在 [20] 中,他们使用 1D-CNN 自动学习加密流量的特征,这比 2D-CNN 更适合加密流量分类的任务。结果表明,1D CNN 的分类性能得分普遍高于 C4.5。殷等。 [21] 使用递归神经网络 (RNN-IDS) 探索了基于 DL 的入侵检测系统。结果表明,在二分类和多分类任务中,RNN-IDS 的性能优于传统的 ML 分类方法,包括 J48、人工神经网络、RF、SVM 以及前研究人员研究的其他 ML 方法。

DeepDefense [49] 结合了 RNN 和 CNN 将基于 DDoS 数据包的检测转换为基于窗口的检测。与传统 ML 相比,错误率大大降低。然而,DeepDefense 的训练需要大量的参数并且耗时较长。近年来,[50] 中提出的 Lucid 考虑了资源受限设备的轻量级部署,并使用 CNN 共享卷积核的权重参数,以减少模型所需的存储空间。实验表明,Lucid 可以在测试数据集上使用低复杂度模型实现高分类准确率。上述研究表明,使用 DL 的流量分类性能可能优于传统 ML,轻量级模型也应作为衡量模型性能的标准。

## B. NAS

大量 ML 应用程序依赖于专家学习来预处理数据、准确选择特征、选择合适的模型和优化超参数。即使使用深度学习来训练网络,也需要针对不同的数据集重新选择网络的超参数,甚至需要从头开始设计网络结构。因此,自动化学习的趋势越来越大,它允许在没有人为干预的情况下应用模型。AutoML 应运而生。近年来,AutoML 方法 [39]、[44]、[45] 已经足够成熟,并且在某些任务 [52]–[54] 上实现了与手动设计的网络架构相媲美的性能。作为 AutoML 的一个分支,NAS 的主要任务是选择合适的网络架构。

NAS 已经成为近年来新兴的研究趋势,因为从业者可以不再依赖手动设计的网络,自动生成任务相关的网络。NAS 方法需要通过定义最大数量来参数化搜索空间

层和操作。然后,通过不同的搜索策略学习网络架构,选择性能好的模型。最后,准确评估候选模型或最优模型。因此,以下研究主要集中在搜索空间、搜索策略和模型评估方面。

搜索空间一般有两种定义空间结构的方式:搜索整体结构 (global search) 或搜索单元结构,根据预先定义的大结构将单元拼接在一起 (cell-based search)。在早期的研究[46]、[32]中,全局搜索空间被设计为链式结构或跳跃式结构。

然而,往往需要搜索整个网络架构中的所有组件,缺乏灵活性。使用基于单元的 [26]、[51]、[16]、[39] 搜索空间是开发中的常见选择,以便在搜索结构中实现良好的鲁棒性和有效性。这种方法设计简单,通常由许多重复的单元组成,用于形成更大的架构。结果,搜索空间将大大缩小,搜索架构也减少到搜索单个小区。细粒度搜索空间 (原子块)[51] 将每个块的可选搜索空间限制为卷积的类型、输出通道的数量和卷积核的大小。针对目前的流量分类任务,为了降低模型的复杂度,使结构在数据集之间具有更好的迁移能力,我们在设计中采用了 cell 结构。搜索策略大致可以分为三类,即基于梯度的方法[22]–[24],强化学习 (RL)[46]、[47]、[26]和基于EA的[18]、[27]–[30]方法。模型评价可分为搜索过程中的搜索目标和搜索后的评价指标两个阶段。前者通常通过多个或单个目标来预测候选模型的性能,以确定是保留模型还是在此基础上进行扩展。后者评估搜索后得到的最优模型 (可能堆叠模型形成更深的网络),并通过在相同训练集上与比较模型进行公平比较或将其应用于其他数据集来重新评估模型的性能以证明其可转移性。

目前所有关于 NAS 的工作主要集中在缩小网络搜索空间、寻找尽可能收敛的搜索策略、选择合适的模型评估方法等方面。构建搜索空间 (cell-based search) 主要考虑网络拓扑和操作类型。在以往的研究中,操作的类型通常是固定的,以简化搜索空间。然而,网络的各种拓扑结构应该是讨论的重点。在本文中,我们在传统的流量分类操作的基础上,加入了计算机视觉领域的相关操作,以提高分类精度。我们网络的设置类似于[28]中定义的结构;即块中节点之间的连接是一种操作类型,每个块沿深度线性连接。

我们将搜索空间中的操作数限制为

一个固定值,并根据流分类任务将其简化为只有一层的块。我们还设计了一种特殊的网络结构来减少通道数和空间比。这样一来,目前搜索结构的复杂度已经完全达到了我们的预期。然而,使用低复杂度结构找到与 [20] 相当的分类精度已成为一个更值得注意的问题。换句话说,找到的架构应该始终考虑准确性和冗余内存消耗之间的隐式权衡。我们介绍 NSGA Net,这是一种由 Lu等人提出的基于遗传算法的网络架构搜索方法。[27],通过父代交叉和继承提取PS。这样,我们就可以同时衡量网络的复杂度和准确率,从而做出最终的选择。受此启发,我们还考虑了另外两种类似于 NSGA-II 的优化算法来寻找任务匹配搜索策略。

### C. MOAs

随着全局优化问题的日益复杂,专家们更加关注多目标求解问题。在此类问题中,优化目标函数在多种因素的相互制约下导致计算量急剧增加。规划算法、分支定界算法等确定性算法已经无法解决复杂的生产和生活需求。智能进化算法 (IEA)的出现解决了这个问题。它利用模拟生物学的遗传规律来解决高度复杂的非线性问题。根据不同的科学技术,多目标 IEA 可以分为基于 Pareto 的、基于聚合的和基于指标的。[61]在原有方法的基础上提出了SPEA-II,解集的收敛性和多样性更好。Coello 和 Lechuga [62] 提出了一种基于 Pareto 的 MOPSO 算法。在迭代过程中,外部存档用于存储非支配解,结合其他种群成员引导粒子飞行。它具有易于实现和快速收敛的优点。DEB[63]团队提出的NSGA-II成为近年来多目标优化算法的研究热点。随后,DEB团队摒弃了NSGA-II中的拥挤距离策略,引入广泛分布的参考点来处理个体分析中多于三个目标的优化问题,从而提出了NSGA-III[64]。NSGA-III解决了NSGA-II在高维目标优化任务中收敛性差、多样性低的问题。[65]提出了基于分解的多目标进化算法 (MOEA/D)算法,该算法在高维多目标求解中具有更好的性能。随着多目标优化问题中目标维数的增加,基于指标评估框架的EA被开发出来,如ISDE+[66]、HypE[67]和MAOE/IGD[68]。

NSGA-II、MOPSO 和 SPEA-II 广泛用于 MOEA。然而,在过去的研究中尚未测试许多多目标测试问题的性能。

事实上,在考虑MOEA应用的过程中,我们综合比较了以下几种情况: NSGA-III、MOEA/D等算法需要大量的尺度向量或合适的参考集,不易应用在现实世界中的问题 [72]。我们的任务只包含两个优化目标,这不是一个高维目标优化问题。近年来提出的很多算法,如ISDE+、MAOA/IGD等基于指标的算法,都比较关注高维目标的情况,本文无需过多关注。没有事实可以否认MOPSO、NSGA-II 和 SPEA-II 算法在解决实际问题中的有效性。相反,将实验设计方法与这些 MOEA 相结合是多目标任务的常见解决方案。

由于 PSO 在处理大规模复杂问题方面的良好性能,研究人员经常使用 MOPSO 来解决计算时间长的多目标优化问题 [69],[70]。SPEA-II 和 NSGA-II 是 MOEA 中常用的算法。[71] 提出 SPEA-II 作为求解最大化智能电网利润的 Pareto 解集的基本框架。在 [56] 中,NSGA-II 和 SPEA-II 算法被应用于智能电网环境以管理峰值负荷调度问题。结果表明,两种算法都具有良好的收敛性,但NSGA-II在时间复杂度和精度上表现更好。

基于以上分析,我们使用NSGA-II算法实现基于NAS的流量分类问题,并将结果与SPEA-II和MOPSO进行比较。

### 三.方法

对于流量分类,在实际应用中,受制于庞大的实时流量和有限的硬件资源,必须考虑模型的计算复杂度。因此,我们应该平衡多个目标 (例如,预测性能和计算复杂性)。在本文中,我们分别采用 FLOPs [37] 和 F1-score 来判断模型的计算复杂度和分类有效性。通常,当考虑多个目标时,可能没有一个完美的解决方案可以在所有所需指标中达到最佳分数。因此,我们试图在有效性和复杂性之间找到权衡。

我们将三种优化算法,即 NSGA-II、SPEA-II 和 MOPSO 应用于架构搜索,可以自动生成一组有用的 CNN 模型。[38]指出,通过基于小区搜索空间的 NAS 搜索获得的网络收敛速度更快、更稳定。因此,我们在三种优化算法下选择分类性能更小、FLOPs更少的架构,并比较不同架构在验证数据集上的F1-score曲线的收敛性。此外,结合流量分类特征,

我们设计了一个可以提高模型性能的组有子结构。本节的其余部分描述了我们架构的细节。

#### A. 数据处理

在本文中,流量数据包使用十六进制编码表示。我们将原始数据转化为十进制编码,模型直接对数据进行分析。与传统的人工特征工程相比,它为分类模型包含了更多的信息。数据处理如下:

##### 1) 数据清理

首先,我们应

删除冗余和重复的包。

一个流量包一般由以太网层、网络层、传输层和应用层组成。

我们删除以太网层的数据,其中包含 MAC 源/目标地址和协议版本。

另外,IP地址也没什么用。此信息与网络行为无关。

##### 2) DATA SPLIT

此步骤中,我们使用相同的五元组信息(源/目标 IP、源/目标端口和协议)拆分流量数据。具有相同五元组信息的流量包构成一个流。我们使用 SplitCap 工具来拆分流量。

##### 3) 矢量化

我们只使用 10 个数据包作为网络流。少于 10 个数据包的网络流用零填充以达到一定长度。对于每个数据包,我们仅提取 160 字节的有效载荷。当一个数据包没有 160 字节时,我们在它后面填充零。最后,我们将每个交通流转化为一个 1600 维的向量。我们可以将其大小调整为 CNN 可以处理的二维向量。

#### B. 遗传搜索架构

##### 1) ENCODING

从生物学的角度来看,神经网络架构可以看作是一种表型,它是从它的基因型中映射出来的。交叉和变异等遗传操作是在基因型空间中进行的。基因型和表型之间的映射关系在本文中称为编码。[60]中也提到了这种编码映射的想法。

换句话说,我们应该定义神经网络架构的编码。

大多数现有的 CNN 可以被视为定义分层计算的计算块的组合(例如,ResNet 块 [13]、Inception 块和 SE 块)。我们遵循 Xie 和 Yuille [32] 提出的编码方法。然而,现有的架构(例如, Alexnet [41] 和 GoogLeNet [42])是使用图像处理进行搜索的,这需要更深更大的网络来处理复杂的场景。流量分类更容易

区分,更深的网络可能会导致过拟合。

因此,我们应该减少任务的搜索空间。

首先,我们将整个分类模型分为几个阶段,如 [39]、[40] 中所述。每个阶段都是一个由几个基本操作组成的块。要对整个网络进行编码,应首先对块进行编码。

块编码:我们提出的二进制网络表示将网络架构编码为二进制字符串,用于指定流出节点的数据流是否需要减少通道数或改变空间比。种群中的网络架构称为块,块由描述操作的若干节点组成。这里,节点是一个基本的操作单元,可以是单个操作,也可以是一系列操作。

这样,我们就可以用几个块的组合来表示一个网络。这些块可以看作是基本操作的组合。在本文中,为简单起见,我们的最终网络重复相同的块。给定第  $i$  个块  $x_i$  作为一部分,表示为  $x_i = (x_i^1, x_i^2, \dots, x_i^N)$ , 其中  $x_i^k$  和  $x_i^N$

操作集由搜索空间定义。该集合总共包含 10 个操作,从中随机选择一个操作作用于当前节点的流出。此外,对于有流量流出的节点,我们通过编码判断该节点是否需要改变通道数。网络  $k$  架构中第  $i$  个块的第  $k$  个节点定义为  $x_i^k$

我。因此,

$$x_i^k = \begin{cases} CHI, CHO \rightarrow CHI, CHO/nBN, & \text{如果 } k = 0, 1 \\ CHO, CHI \rightarrow CHO, I/nBN, & \text{否则。} \end{cases} \quad (1)$$

其中  $k = 0, 1, 2, \dots, L$ ,  $L$  表示区块中  $k$  个节点的个数。如果节点  $x_i$  连接到编码为 0 或 1 的节点  $i$ ,则适用于操作

$k \times i$  的流出不会改变,而输出通道

CHO 减少到  $1/nBN$ 。  $nBN$  表示空节点的个数(即除了 Concat 或 add 之外没有对该节点进行任何操作)。但是,如果当前节点连接到 0 和 1 以外的节点,则对该节点的流出流量进行运算的输入输出通道数减少为  $1/nBN$ 。图 1 显示了由一个块组成的完整网络架构。

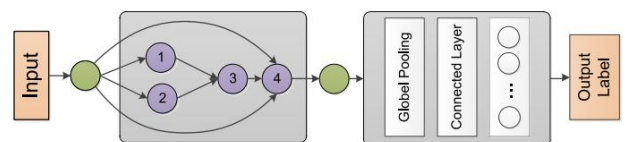


图 1. 一个分类网络包含一个带有 4 个节点的块。

搜索空间:为了使架构搜索更容易,我们应该预先确定块之间的输入层、输出层和连接层。块的总搜索空间由操作数和



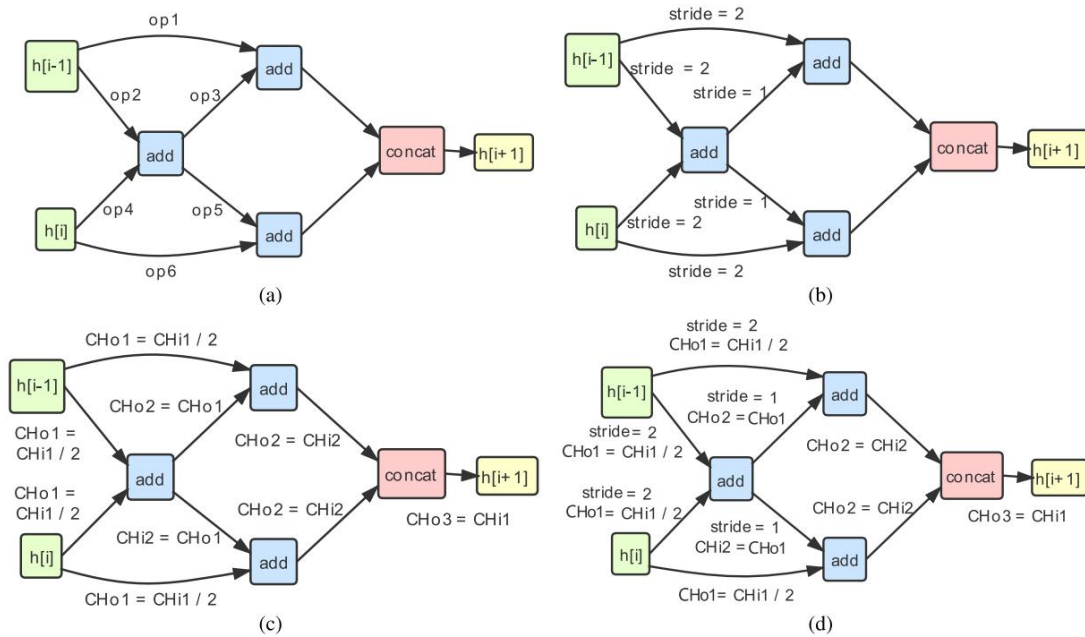


图 2. (a) 具有完整操作集的架构。(b) 空间比例下降。(c) 渠道数量减少。(d) 空间比率和通道数量的减少。

节点数。块的搜索空间为：

$$x_i^k = \prod_{m=1}^{m=\text{否}} ((m+1)2)^{n_p^{\text{否}}} \quad (2)$$

其中 $n_p$ 是操作数， $n_o$ 是块中的节点数。因为我们将不同阶段的编码设置为相同，所以一个完整网络的搜索空间相当于一个块。

为了丰富我们的搜索结果并提高网络性能，我们添加了一些预定义的架构块。

下一节将详细讨论建议的预定义架构。

2) 预定义架构块在本节中，我们预定义了一些有用

的块，这些块具有较低的空间比和较少的通道。我们还测试了该架构的轻量级和运行速度，并将其与手工设计的 CNN 模型进行了比较，证明该架构在预定义的搜索块中更轻、更快。在我们的论文中，普通块是有向无环图。

原始架构：首先，与之前手工制作的网络相比，我们仅使用原始操作，如 2D 卷积和池化。在图 2 中，我们展示了一个块的完整结构。卷积运算是块中的边缘。块中的节点有两个输入，我们使用 add 合并两个输入。最后，Concat 操作有选择地组合先前节点的信息以进行输出。原始操作集由 ReLUConvBN、MaxPooling、AvgPooling 和 Skip 组成。详细结构如图3所示。

Architecture With the Full Operation Set:最近，一些更有效的卷积运算被提出。

例如，为了在不改变特征图的空间比例的情况下提取更详细的信息并扩大感受野，我们将扩张卷积操作添加到全操作集。为了解决训练过程中梯度消失的问题，在操作集中引入了ReLU非线性函数作为激活函数，并在部分操作中加入了batch normalization。Sep Conv 使用水平和垂直两个卷积核来替换原来的卷积核。我们向操作集中添加一些新操作以构建新块。

图 3 显示了新操作的详细结构。

**降低空间比：**对于卷积网络，降低特征图的空间比可以降低计算复杂度并整合低级信息。因此，我们将操作集中卷积操作的步幅从1改为2。然后，特征图的空间大小将在经过一个块后减半。我们在图 2 中显示了原始块和空间比率降低的块之间的差异。

**减少通道数：**除了减少空间比外，减少运算的通道数也是有效的。块中的不同路径可以看作是不同的信息流。那么，减少信息流的通道数就意味着压缩信息。最后，该操作作用于组合所有信息流。在此设置中，我们保持块的输入和输出之间的通道数量相等。我们称连接到输出节点的节点为**空节点**。然后，我们将输入和输出节点之间的节点数设置为  $M$ ，使得空的数量

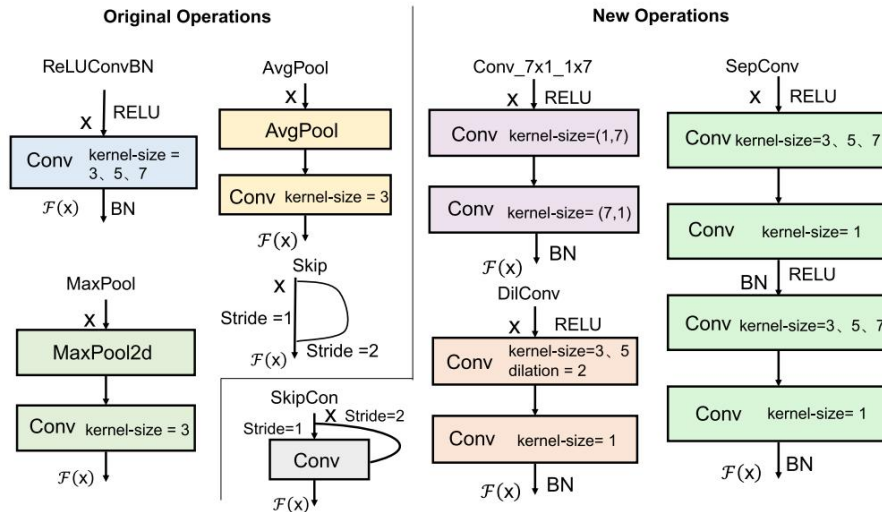


图 3.主要操作的详细实施。左侧包含流量分类中的常用操作,右侧增加了矩形卷积、深度可分离卷积、扩张卷积和跳跃连接。

节点是  $[1, 2, \dots, M-1]$ 。因此,输出通道数应该是  $[1, 2, \dots, M-1]$ 。

图 2 显示了具有较少通道的块的详细结构。

**空间比率和通道数量的减少:**接下来,我们可以构建一个空间比率和通道都减少的块。图 2 显示了这种块的结构。

除了以上四个设计块,我们希望进一步扩大搜索空间,找到更好的结构。

因此,我们设计了两组搜索空间:**固定初始通道**和**搜索初始通道**。由于前者只是简单地指定了原始的通道数,因此设置值将在第4节中描述。这里只介绍后者的相关原理。

Searching for Initial Channels:通过将初始通道数从原来的固定值修改为可变通道数来扩展搜索空间。第一代的初始种群长度修改为  $(Length_{fixed} + 1)$  ,其中 $Length_{fixed}$ 为固定通道数条件下的初始种群长度。

网络架构代码的最后一个值表示可搜索的通道值,我们将其设置为 12、24、36 和 48。

### 3) 搜索程序经过几千年的进

化,自然界万物的存在必须被证明是合理的。人们寻求自然界的最优法则并将其发展为 EA。NSGA-II、MOPSO 和 SPEA-II 是基于自然优化规则的 MOEA。在当前任务中,我们规定个体的每一位都必须是整数;因此,整数规划问题值得关注。当种群中的个体发生交叉变异时,本质上是个体中的一个位和一个范围为(0,1)的随机数

即加减。因此,修改后的代码通过舍入重新映射为整数。这三种优化算法的细节如下:

- 1) NSGA-II 这是一个解逐渐变好的过程。首先,我们随机初始化几个网络架构,称为种群。在每次迭代中,新的网络架构由从种群中采样的父网络生成,包括变异和选择过程[55]。每个网络都为生存和繁殖(成为父母)而竞争。经过几代之后,种群中的网络将获得该数据集的 PO。

NSGA-II 中的突变和选择过程描述如下:

**突变:**为了增强种群的多样性 (具有不同的网络架构)和逃离局部最优的能力,我们随机翻转位编码。为了防止创建完全不同的架构,我们将每个变异操作的翻转位的数量限制为一个。

选择:生成网络架构后,我们使用统一的度量来选择有效网络。在流量分类任务中,我们使用 FLOPs 和 F1-score 来选择网络。

## (2) SPEA-II 与

NSGA-II 相比, SPEA-II 的运算效率较低, 但能够更好地解决高维优化问题。此外, 赫斯坦等人。[43] 表明 SPEA-II 在约束和无约束多目标优化问题上都比 NSGA-II 具有更好的性能。以下是 SPEA-II 中的关键步骤, 首先初始化一个用于存储历史世代的档案集 At 和一个用于当前世代的种群集 Pt。环境选择策略在 At 和 Pt 中实施, 以生成生成的 At+1 和 Pt+1。

然后,对新形成的 $At+1$ 和 $Pt+1$ 的个体进行变异操作。环境选择策略的具体实现过程如下:

环境选择策略:帕累托最优解 (nonnormalized soluitons)的特点是不能在提高任何目标函数的同时削弱至少一个其他目标函数。非支配解选自 $Pt$ 和 $Et$ 。

非支配解集保存在下一代存档种群 $Et+1$ 中。如果 $Pt$ 和 $Et$ 的非支配解集中的解数小于 $Et+1$ 的大小,则将 $Pt$ 和 $Et$ 中支配程度较低的优势个体保存在 $Et+1$ 中,以维持种群多样性。然而,当非支配解的数量大于 $Et+1$ 的大小时,基于 $k$ 近邻的截断策略遵循以保持外部种群的大小。

### (3) MOPSO

在MOPSO中,将多目标优化问题的每一个解看成一个粒子,每个粒子的当前位置由一个适应度函数表示。而且,每个粒子都可以记住自己的历史最佳位置,并根据自己的经验和种群中的其他粒子选择飞行方向和距离。为了将粒子引导到 Pareto 前沿 (称为全局最优),需要更新粒子的位置和速度,如下所示:

$$v_i = \omega v_{io} + c_1 r_1 (x_{p\_best} - x_{io}) + c_2 r_2 (x_{g\_best} - x_{io}) \quad (3)$$

$$x_i = x_{io} + v_i \quad (4)$$

其中 $v_{io}$ 和 $x_{io}$  ( $0 \leq i < N$ )是速度,位置是最优的

当前一代的粒子我,分别。  $x_{p\_best}$

第  $i$  个粒子到达的位置,  $x_{g\_best}$

种群中所有粒子到达的位置。  $c_1$ 和 $c_2$ 是两个加速度系数,  $r_1$ 和 $r_2$ 是两个随机数。  $\omega$  表示如下:  $t \times (\omega_{max} - \omega_{min}) + 1$

$$\omega = \omega_{max} - \frac{t \times (\omega_{max} - \omega_{min})}{\text{最高温度}} \quad (5)$$

较大的  $\omega$  有利于粒子跳出局部最优。然而,较小的  $\omega$  有利于算法的收敛。我们将  $\omega$  的初始值设置为 1,并使用上面的公式将  $\omega$  的直线性减小。  $t$ 代表当前迭代次数,  $t_{max}$ 代表总迭代次数,  $\omega_{max}$ 为全一D维向量,  $\omega_{min}$ 为零D维向量。  $D$ 是每一代粒子的编码长度。粒子的初始速度是随机的。

与前两种方法类似,MOPSO也是一种迭代优化算法,但在实现过程中没有交叉或变异。

### C. 轻量级模型

由于存储空间和功耗的限制,神经网络模型在

嵌入式设备的存储和计算。我们从基本的卷积运算开始,以在不牺牲网络性能的情况下降低计算复杂度。

MobileNet V1 和 V2 以及 shuffle Net V1 使用 FLOPs 评估模型维度,因此我们为 NSGA-net 搜索的最终网络计算 FLOPs。我们通过以下两种方式减少 FLOPs:1)在 MobileNet V1 之后,我们使用深度可分离卷积代替标准卷积来减少参数数量。

2)我们设计了一个网络架构来同时减少通道数和空间比。减少通道数量可以获得更轻量级的模型,降低空间比例可以降低模型复杂度。

评估模型的复杂性使用 FLOPs、MAccs 和模型推理能力来衡量。此外,使用模型参数和内存使用情况评估模型的轻量级。

## 四、实验

在本节中,我们将解释网络结构的参数设置和实现细节。实验分为三个部分。首先,将基于NSGA-II的优化算法应用于之前设计的五个搜索空间,进行消融实验,选择效果最好的一个。在这一部分中,我们重点比较哪个搜索空间可以找到更好的模型,因此我们只选择 NSGA-II 作为搜索策略。

其次,比较三种优化算法在选定搜索空间的性能,然后基于三种优化算法从帕累托最优集中选择三种结构。最后,通过比较 MAccs 和 F1-score 曲线来分析所搜索架构的轻量化和速度性能。更多详细信息,请参见以下说明:

### A. 实施细节

数据说明:为了验证搜索的有效性,我们选择了两个公共数据集。我们使用 IDS2012 数据集来检测入侵流量。该数据集包含不同类型的恶意软件流量,包括暴力 SSH、DDoS、HTTPDoS 和中继攻击。分析该数据集的难点在于不同流量的分布不均衡,如表 1 所示。为了证明该搜索策略能够以比人工设计的不同数据集更好的性能搜索网络架构,我们重新运行了实验在 ISCX VPN 数据集上。

这个数据集有 7 个一般类别的加密流量,即网页浏览、电子邮件、聊天、流媒体、文件传输、VoIP 和 P2P,如表 2 所示。我们拆分两个原始训练集来创建我们的训练 (70%)和验证 (30%) 集用于架构搜索。最后,当架构完全重新训练时,测试结果由原始分区数据集得到。

超参数:网络架构仅由一个块组成,其中每个架构中没有重复模式。在我们的设计中,每个块包含



表 1. IDS2012 数据集描述。

Class Name	Quantity	Percentage(%)
Normal I	8483064	95.323
Brute Force SSH	6964	0.78
DDoS	21121	2.37
HttpDoS	3482	0.39
Infiltrating Transfer	10044	1.13
TOTAL	998817	100

表 2. ISCX VPN 数据集描述。

Class Name	Description	Quantity	Percentage(%)
Email	SMTPS, POP3S and IMAPS.	26844	14.94
Chat	ICQ, AIM, Skype, Facebook and Hangouts.	33978	18.92
Streaming	Vimeo and Youtube.	26682	14.85
File Transfer	Skype, FTPS and SFTP using Filezilla and an external service.	30000	16.7
VoIP	Facebook, Skype and Hangouts voice calls.	30000	16.7
P2P	uTorrent and Transmission (Bittorrent).	32130	17.89

6 个操作和 5 个节点。5 个节点中,2 个节点为固定节点 (图1中标记的0 号和1号节点),其余3个节点为6个随机生成操作的中间连接节点。最后将所有中间连接节点的输出数据流拼接在一起作为输出结果。因此,我们将块数设置为 1,将节点数设置为 3 (两个固定输入节点除外)。我们将随机种子设置为0,并使用均匀分布的随机数确定第一代的初始种群,以确保每个实验都以相同的随机数开始迭代。世代数为10,每代种群规模为20;因此,每次搜索可以获得 200 个后代,这在 PyTorch 中的 NVIDIA 1080Ti GPU 上大约需要 2-3 天。

训练细节:对于每个卷积块,我们在训练集和测试集中训练 12 个 epoch,批量大小为 128。然后,我们使用动量随机梯度下降 (SGD) 优化权重并使用余弦退火调整学习率。在循环学习率结束时,初始学习率为 0.025,可以降低到 0。我们将动量设置为 0.9,权重衰减为  $3 \times 10^{-4}$ 。

在NSGA-II中,交叉概率和变异概率都设置为0.4。在 SPEA-II 中,存档大小设置为 20。

B. 消融实验

为了研究不同输入通道数对模型分类性能和复杂度的影响,我们设计了两组对比实验:固定初始通道和搜索初始通道。

在具有固定数量的初始通道的实验中,我们在五个不同的搜索空间中进行消融实验。我们发现基于原始操作在搜索空间中找到的结构结果并不理想;因此,在搜索初始信道实验时,只选择最后四组搜索空间。

表 3 显示了每个搜索空间的 Pareto 最优解表示模型的性能。使用原始操作的原始架构要复杂得多。随着更多操作的添加,模型性能得到改善。因此,新操作也适用于流分类。

空间比降低的结果如表 3 所示。很明显,F1 分数增加而 FLOP 减少。降低特征图的空间比例可以聚合中间特征,降低计算复杂度。根据通道缩减数据,我们发现如果仅仅减少通道数量,并不能显着提升模型的性能。但是,如果同时降低空间比和通道,如表中粗体所示,这个搜索空间可以找到一个F1-score更高的网络结构。

为了证明我们的结果不是偶然的,我们将分析整体趋势如下。图 4 显示了 NSGA-II 在不同实验组中基于双目标得到的散点图。该图清楚地显示了四组消融实验下整个人口的改善。在full operations的实验中出现了大量的outliers,在图5的box diagram中体现得比较清楚,说明在full set的操作中搜索出了很多双目标不理想的架构。在仅降低空间比的搜索空间中,F1-score 和 FLOPs 的异常值大大减少,同时它们的指标得到改善。对于减少通道数的方法,F1-score 得到改善,异常值减少,但模型往往更复杂。然而,降低空间比和通道数的方法可以大大提高 F1-score。

此外,输入通道的初始数量可能会有所不同。我们可以将初始输入通道添加到搜索空间。增加搜索初始输入通道数的结果如图6所示,可以看出四组搜索空间的FLOPs值较固定初始通道有明显增加,整体 F1 分数也有所提高。无论是从PO中的个体比较 (表3)还是整体搜索结果 (图6)来看,降低空间比后FLOPs都有明显的下降,同时降低空间比后F1-score也有所提高和号码

表 3.两组实验中的最佳结构（训练 12 个 epoch 后的结果）。

		FLOPs(MB)	F1-score(%)	Accuracy(%)	Precision score(%)	Recall score(%)
Fixed initial channels	Original architecture	33.005	99.227	99.223	99.201	99.252
	Architecture with full operation set	18.413	98.968	98.961	98.931	99.005
	Decrease in spatial ratio	7.133	99.448	99.446	99.430	99.464
	Decrease in channels	18.873	98.870	98.863	98.832	98.917
	Decrease in spatial ratio & channels	11.501	99.574	99.573	99.560	99.586
Searching for initial channel	Architecture with full operation set	198.068	99.680	99.679	99.670	99.688
	Decrease in spatial ratio	44.467	99.660	99.656	99.650	99.671
	Decrease in channels	204.058	99.564	99.563	99.550	99.577
	Decrease in spatial ratio & channels	52.762	99.787	99.786	99.780	99.792

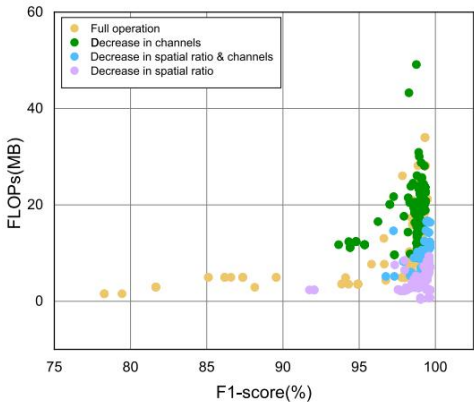


图 4.基于 IDS2012 数据集的四组消融实验中人口双目标的改进。

渠道。上述结果表明,我们设计的搜索空间在降低复杂度和提高分类性能方面是有效的。这个结果在图 7 中更加直观。随着初始通道数的增加,F1-score 和 FLOPs 都有不同程度的提高。

以上实验结果总结如下:在可变初始通道方法中,虽然模型的F1-score 比较高,但是复杂度也增加了更多。此外,我们发现当通道数增加时,模型的复杂度和 F1-score 都是理想的

为12。因此,在通道数固定为12的情况下,我们考虑将搜索空间扩展到全集操作,并在通道数和空间比减少的操作空间上进行后续实验。

C. 关于搜索策略的结论

在本节中,我们采用不同的优化算法来降低空间比和信道搜索空间来选择最佳搜索策略。我们采用了第 II 节中介绍的 3 种优化算法,可以自动搜索在错误（错误 = 100 - F1 分数）和恶意流量分类任务的复杂性之间近似 Pareto 前沿的结构。从图 8b 可以清楚地看出,第 10 代

使用MOPSO搜索结构,每一代的FLOPs都很低（初始代的FLOPs低于其他两代）。MOPSO 在搜索低复杂度架构的任务中表现良好。

然而,就PS中的结构数量而言,如图8a所示,NSGA-II算法比其他两个多（红点代表Pareto最优结果）。

从8c我们观察到SPEA-II无法搜索到FLOPs小于2.5Mb的结构,POs的数量也是最少的。

由于结构的复杂度普遍较低,MOPSO算法的实现也比较简单,如表4所示,三种优化算法中运行时间最短的是MOPSO算法,其次是NSGA-II, SPEA -II 需要最长的运行时间。图 9 比较了三种优化算法搜索后得到的双目标下每一代 POS 总数的分布。

NSGA-II 更有可能搜索具有高 F1 分数的个体,而 MOPSO 倾向于搜索具有低 FLOP 的个体。此外,表4显示,在三种优化算法搜索的PO中, NSGA-II搜索最高的F1-score,MOPSO搜索最低的FLOPs。此外,从图 9 看,NSGA-II 和 SPEA-II 搜索到的 PO 相对聚集,而 MOPSO 搜索到的 PO 更加分散。我们分析了可能的原因如下: NSGA-II 和 SPEA-II 存在遗传交叉,突变,种群之间共享的信息紧密,因此这两种算法搜索到的模型中异常值的数量相对较少。另一方面,MOPSO 遵循单一的信息共享机制。虽然粒子能以很快的速度收敛,但它们之间的关系并不密切,因此存在很多离群值。

为了进一步比较三种算法搜索的 PO 的性能,描述了在验证数据集上测量的 F1 分数曲线。图 10 显示基于 NSGA-II 的搜索块在第 40 个 epoch 左右出现短暂的震荡,但随着训练的进行趋于稳定;同时,其他两个模型的F1-score曲线出现了大幅震荡。此外,NSGA-II 还搜索了

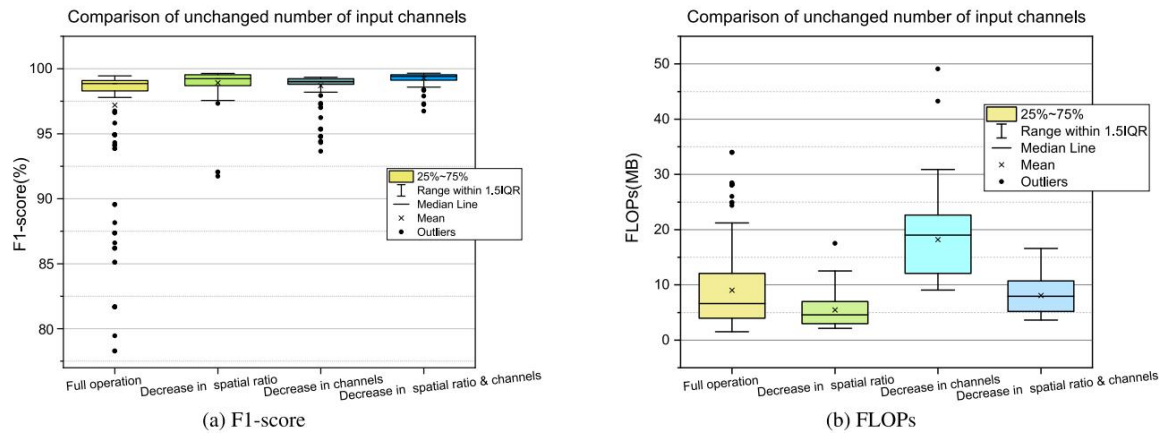


图 5. 基于 IDS2012 数据集的具有固定输入通道数的四组实验的箱线图。

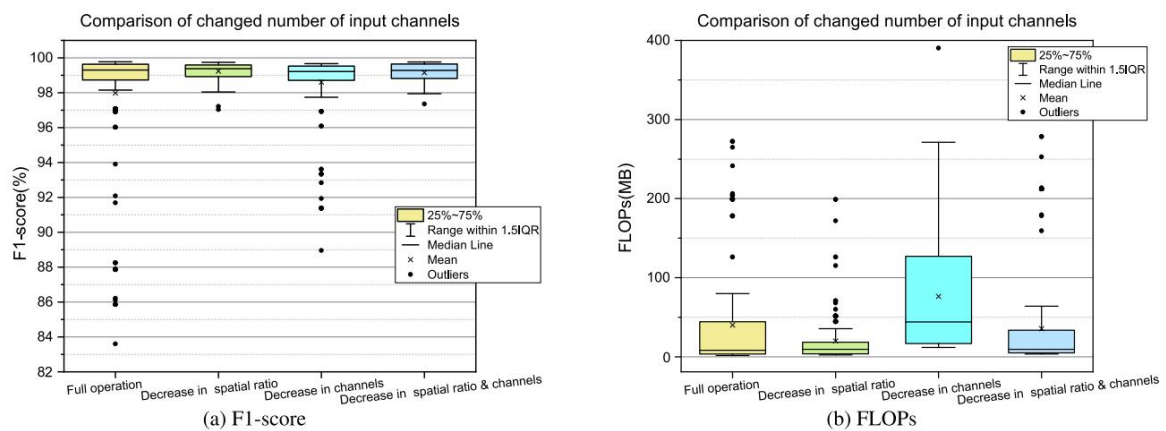


图 6. 四组实验的箱线图以及基于 IDS2012 数据集的搜索输入通道数。

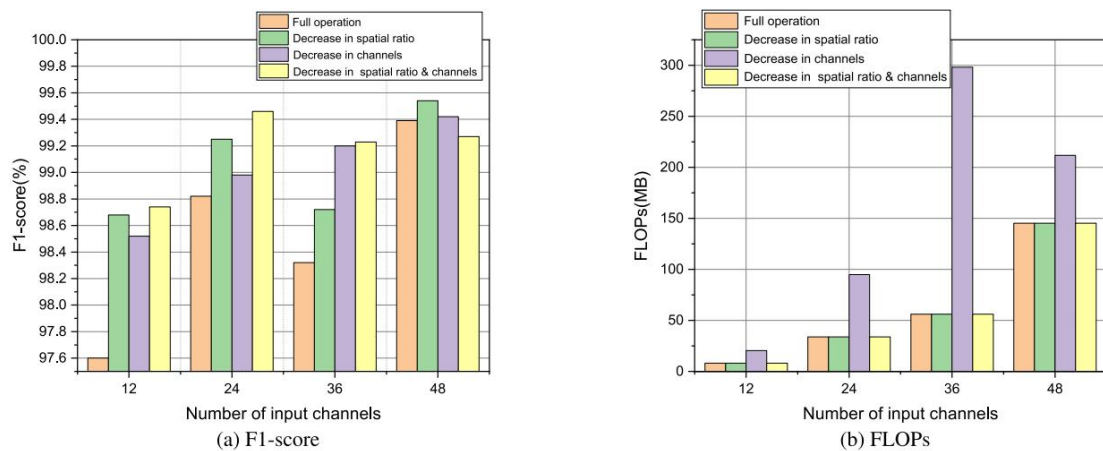


图 7. 四组实验的条形图以及基于 IDS2012 数据集的搜索输入通道数。

模型在训练第 50 个 epoch 后趋向于具有小的收敛误差和小的阻尼振荡,而其他两个模型仅在大约第 70 个 epoch 后才收敛。这一结果表明 NSGA-II 得到的模型比其他模型具有更好的稳定性和收敛性。

#### D. 架构评估

我们搜索到的基于 NSGA-II 的架构的 F1 分数已经超过了手工设计的架构。然而,在恶意流量检测中,需要通过实时检测及时阻止恶意流量。此外

对于 F1 分数,计算复杂度是另一个

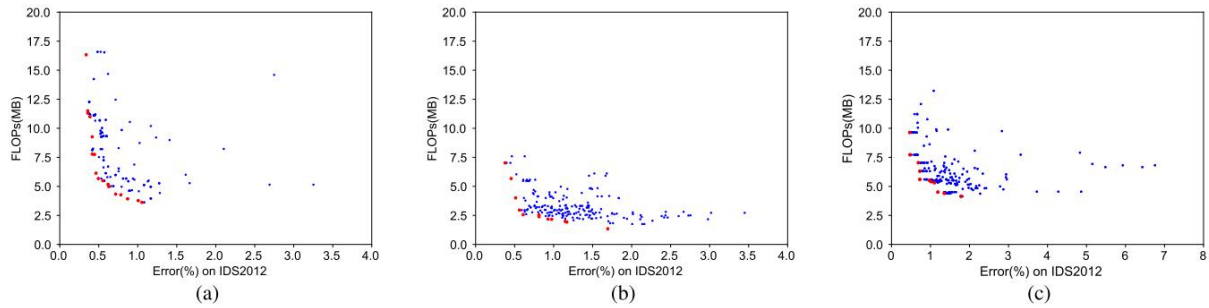


图 8. (a) NSGA-II 的权衡边界 (Pareto 最优集包含 17 个最优解)。 (b) MOPSO 的权衡边界 (Pareto 最优集包含 12 个最优解)。 (c) 基于 IDS2012 数据集的 SPEA-II 权衡边界 (Pareto 最优集包含 11 个最优解)。

表 4. 与不同优化方法的比较。这张表中,每一个最优解都是从 Pareto 最优解集中选出的, F1-score 是基于 IDS2012 数据集训练 120 个 epoch 的结果。

Methods	F1-score(%)	FLOPs(MB)	GPU Hours
MOPSO	99.699	2.959	10
NSGA-II	99.806	11.501	20
SPEA-II	99.738	5.597	25

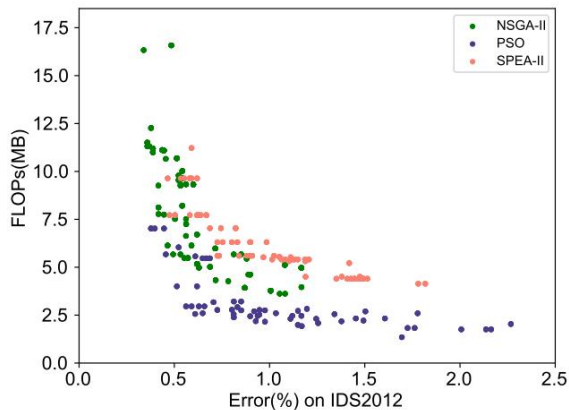


图 9. 基于 IDS2012 数据集的优化算法的帕累托最优结果。

表 5. 不同 EA 算法下搜索模型的复杂度、参数数量和速度的比较。

Methods	Params(KB)	MAcc(MB)	Flops(MB)	GPU Speed (Batches/sec.)
NSGA-II	25.510	22.18	11.3	28.962
MOPSO	9.557	5.68	2.96	30.789
SPEA-II	11.009	10.71	5.59	20.034
CNN	52.106	54.05	26.99	2.012

CNN 网络要考虑的重要指标。

为了满足这一要求,下面对三个搜索模型在模型复杂度和速度方面的性能进行了评估。

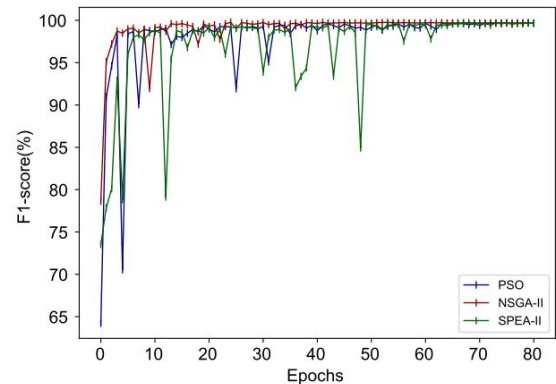


图 10. 训练期间基于 MOPSO、NSGA-II 和 SPEA-II 的架构在 IDS2012 数据集上的验证 F1 分数 (%) 曲线。

在评估模型的复杂度,即模型的计算量时,我们采用了朴素的求解方法。在以往的搜索空间设计中,有很多卷积运算块,其中包含了大量的点乘和累加形式。因此,除了 FLOPs,我们还使用 MACcs 来衡量模型的计算量。

通过计算模型的参数个数来评价模型的轻量化。为了使模型尽可能轻,我们减少了进入卷积核的输入通道数。为了评估模型速度,我们使用更直观的比较方法来比较推理实验的结果。

最终的对比结果如表 6 所示。很明显,使用 NAS 搜索到的模型在模型复杂度和运行速度上都优于手工设计的模型。

在表 6 中,可以使用 MACcs 和 FLOPs 来间接评估模型速度,我们使用推理实验直接测量模型在 GPU 上的运行速度。直观上,模型的 FLOPs 越高,模型的复杂度越高,会导致运行速度越慢。基于 MOPSO 的模型复杂度最低,运行速度最快。基于 NSGA-II 的搜索模型速度略低于



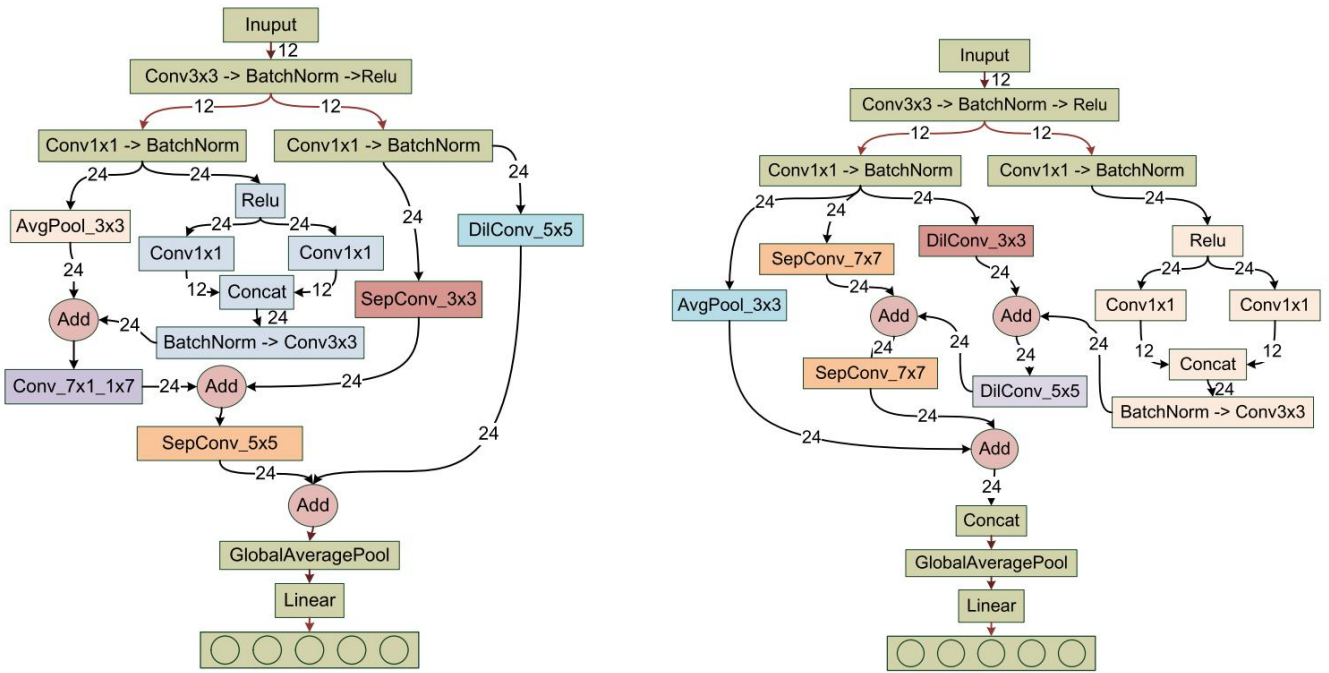


图 11.基于 NSGA-II 在 IDS2012 和 ISCX VPN 数据集上搜索的最佳架构。

表 6.在我们设计的搜索空间中通过 NSGA-II 搜索获得的 Pareto 最优解（降低空间比和通道数）与其他分类算法在 IDS2012 和 ISCX VPN 数据集上的比较。

Dataset	Method	FLOPs(MB)	F1-score(%)	Precision score(%)	Recall score(%)
IDS2012	CNN	26.995	98.96	98.96	98.96
	CNN + Metric Learning	28.363	99.71	99.71	99.71
	KNN	-	95.862	95.932	95.825
	LR	-	54.191	74.827	60.890
	RF	-	97.679	97.616	97.754
	DT	-	97.258	97.317	97.204
	XGBoost	-	97.637	97.813	97.489
	NAS	11.501	99.806	99.802	99.809
ISCX VPN	CNN	12.372	95.43	95.58	95.48
	CNN + Metric Learning	12.995	98.56	98.53	98.53
	KNN	-	98.56	98.53	98.53
	LR	-	68.12	67.19	67.19
	RF	-	23.99	20.25	22.80
	DT	-	85.57	85.21	84.91
	XGBoost	-	84.88	84.04	84.16
	NAS	4.718	99.369	99.374	99.321

NSGA-II。但是基于SPEA-II的模型不是最复杂的,但是运行速度是最低的。在对ShuffleNet V2的研究中[36]表示,模型复杂度并不是影响模型速度的唯一因素,内存访问成本（MAC）也很重要。

也就是说,分组卷积可以减少模型的参数,但是会减慢运行速度。

SPEA-II搜索到的模型中有很多packet convolutions（多于其他两个模型）,降低了模型速度。

E. 与其他模型的比较

以上分析表明,选择空间比小、通道数少的搜索空间是最好的,

并使用 NSGA-II 作为搜索策略。因此,我们在训练集上从头开始训练搜索到的架构。

ML 分类算法 (KNN,LR,RF,DT 和 XGBoost)和两个手动设计的 CNN 网络模型在 IDS2012 和 ISCX VPN 数据集上进行训练。结果如表5所示。从表中可以看出,搜索得到的网络在分类和模型复杂度方面都有很好的表现,所以设计的搜索空间是适用的,搜索策略在这个任务中表现良好。

图 11 显示了搜索到的最佳架构。

## 五、结论

本文研究了基于NAS的流量分类模型。为了进行网络搜索,我们使用 NSGA-II 设计了流量分类网络搜索架构,并将结果与 SPEA-II 和 MOPSO 进行了比较。首先,我们进行了消融实验来证明设计的搜索空间是有效的,减少空间比和通道数的搜索空间可以根据他们的 FLOPs 和 F1-score 搜索 PO。其次,在最优搜索空间改变搜索策略,基于三种优化算法评估模型的准确率和搜索次数。得出结论,NSGA-II搜索的模型F1-score最高,MOPSO搜索模型可以节省时间和精力,SPEA-II搜索的模型F1-score最低。最后,我们设计了相同GPU条件下的推理实验,证明了MOPSO搜索模型的复杂度最低,运行速度最快。当搜索时间和复杂度差异不大时,我们认为加权 F1-score 是最重要的指标,NSGA-II 获得的 PS 中最优解的数量最多。因此,NSGA-II 比其他两种优化算法更适用于流量分类问题。在上述所有情况下,所得模型的加权 F1 分数和速度都超过了人工设计的模型。

## 致谢

作者感谢编辑和匿名审稿人提出的提高论文质量的建议。AJE 在首次提交前对本文进行了完善,相关支持材料在“Supplemental File for Review”中提供。这项工作得到了国家自然科学基金 (61871046) 的支持。

## 参考

- [1] T. Karagiannis,A. Broido,M. Faloutsos and K. Claffy, “P2P 流量的传输层识别”, Proc.第四届 ACM SIGCOMM Conf.,互联网措施。(IMC),意大利西西里岛,2004 年,第 121-134 页。
- [2] N. Weng,L. Vespa and B. Soewito, “自适应入侵检测系统的深度数据包预处理和有限状态编码”, Comput.网络,卷。55,没有。8,第 1648-1661 页,2011 年 6 月。
- [3] D.-W.金,G.-Y.申和 M.-M. Han, “恶意软件分类的特征重要性分析和解释”, Comput., Mater.连续体,卷。65,没有。3,页数 1891-1904,2020 年。
- [4] A Panchenko,F Lanze,A Zinnen,M Henze,J Pennekamp, K Wehrle and T Engel, Proc 中的“Internet 规模的网站指纹识别”。网络。分发。系统。安全。症状。美国加利福尼亚州圣地亚哥:IEEE 计算机协会,2016 年,第 1-15 页。
- [5] R. Dubin,A. Dvir,O. Pele and O. Hadar, “我知道你最后一分钟看到了什么 加密的 HTTP 自适应视频流标题分类”, IEEE Trans.信息。取证安全,卷。12,没有。12,第 3039-3049 页,2017 年 12 月。
- [6] VF Taylor,R. Spolaor,M. Conti and I. Martinovic, “通过加密网络流量分析进行稳健的智能手机应用程序识别”, IEEE Trans.信息。取证安全,卷。13,没有。1,第 63-78 页,2018 年 1 月。
- [7] M. Conti,L.V Mancini,R. Spolaor and NV Verde, “分析 Android 加密网络流量以识别用户操作”, IEEE Trans.信息。取证安全,卷。11,没有。1,第 114-125 页,2016 年 1 月。
- [8] A. Krizhevsky,I. Sutskever and GE Hinton, “使用深度卷积神经网络的 ImageNet 分类”, Proc.进阶神经网络信息过程。系统。(NIPS), 2012 年 12 月,第一卷。25,没有。2,第 1097-1105 页。
- [9] Y. Zeng,H. Gu,W. Wei and Y. Guo, “Deep-Full-Range:基于深度学习的网络加密流量分类和入侵检测框架”, IEEE Access,卷。7,第 45182-45190 页,2019 年。
- [10] M. Lopez-Martin,B. Carro,A. Sanchez-Esguevilas and J. Lloret, “Net 使用用于物联网的卷积和递归神经网络的工作流量分类器”, IEEE Access,卷。5,第 18042-18050 页,2017 年。
- [11] C. Thornton,F. Hutter,HH Hoos and K. Leyton-Brown, “Auto-WEKA:分类算法的组合选择和超参数优化”, Proc.第 19 届 ACM SIGKDD Int.会议。知识Discovery Data Mining,美国伊利诺伊州芝加哥,2013 年 8 月,第 847-855 页。
- [12] H. Wallach, “计算社会科学计算机 + 社会数据”, 公社。美国计算机学会,卷。61,没有。3,页。42-44。
- [13] K. He,X. Zhang,S. Ren and J. Sun, “用于图像识别的深度残差学习”, Proc. IEEE 会议。电脑。可见。模式识别。(CVPR),美国内华达州拉斯维加斯,2016 年 6 月,第 770-778 页。
- [14] P. Wang,P. Chen,Y. Yuan,D. Liu,Z. Huang,X. Hou and G. Cottrell, “理解语义分割的卷积”, Proc. IEEE 冬季会议。申请电脑。可见。(WACV),美国内华达州太浩湖,2018 年 3 月,第 1451-1460 页。
- [15] F. Yu,V. Koltun and T. Funkhouser, “扩张残差网络”,载于Proc. IEEE 会议。帐户你要。模式识别。(CVPR),檀香山,夏威夷,美国,7 月。2017,页。636-644。
- [16] H. Liu,K. Simonyan,O. Vinyals,C. Fernando and K. Kavukcuoglu, “高效架构搜索的层次表示”, Proc. 诠释。会议。学习。代表。加拿大不列颠哥伦比亚省温哥华:温哥华会议中心,2018 年,第 13-25 页。
- [17] F. Al-Obaidey,S. Momtahan,MF Hossain and F. Mohammadi, “用于识别不同社交媒体应用程序的基于 ML 的加密流量分类”, Proc. IEEE 可以。会议。电工。工程。(CCECE),加拿大埃德蒙顿,AB,2019 年 5 月,第 1-5 页。
- [18] VA Muliukha,LU Laboshin,AA Lukashin and NV Nashivochnikov, “使用机器学习对加密网络流量进行分析和分类”, Proc.第 23 国际会议。软计算。措施。(SCM),俄罗斯圣彼得堡,2020 年 5 月,第 194-197 页。
- [19] C. Luo,S. Su,Y. Sun,Q. Tan,M. Han and Z. Tian, “基于卷积的恶意 URL 检测系统”, Comput.,Mater.连续体,卷。62,没有。1,第 399-411 页,2020 年。
- [20] W. Wang,M. Zhu,J. Wang,X. Zeng and Z. Yang, “使用一维卷积神经网络进行端到端加密流量分类”, Proc. IEEE 诠释。会议。智能。安全。信息格式。(ISI),北京,中国,2017 年 7 月,第 43-48 页。
- [21] C. Yin,Y. Zhu,J. Fei and X. He, “使用递归神经网络进行入侵检测的深度学习”, IEEE Access,卷。5,第 21954-21961 页,2017 年。
- [22] S. Richard,P. Charles and S. Dawn, “可微分神经网络架构搜索”,载于Proc.诠释。会议。学习。代表。(ICLR)加拿大不列颠哥伦比亚省温哥华:温哥华会议中心,2018 年,第 1-4 页。
- [23] H. Liu,K. Simonyan and Y. Yang, “飞镖:可区分的架构搜索”, Proc.诠释。会议。学习。代表。(ICLR),美国路易斯安那州新奥尔良,2018 年,第 1-13 页。
- [24] R. Luo,F. Tian,T. Qin and T. Liu, Proc 中的“神经结构优化”。第 32 届会议神经网络信息过程。Syst.,加拿大不列颠哥伦比亚省温哥华,2019 年,第 1-12 页。
- [25] M. Tan,B. Chen,R. Pang,V. Vasudevan,M. Sandler,A. Howard and QV Le, “MnasNet:面向移动设备的平台感知神经架构搜索”, Proc. IEEE/CVF 会议。电脑。可见。模式识别。(CVPR),美国加利福尼亚州长滩,2019 年 6 月,第 2815-2823 页。
- [26] Y. Wei,FR Yu,M. Song and Z. Han, “使用自然演员-评论家深度强化学习联合优化物联网的缓存、计算和无线资源”, IEEE Internet Things J.,卷。6,没有。2,第 2061-2073 页,2019 年 4 月。

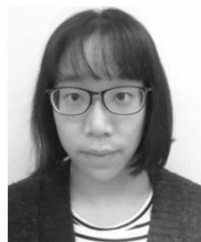
- [27] Z. Lu, J. Whalen, V. Boddeti, Y. Dhebar, K. Deb, E. Goodman 和 W. Banzhaf, “NSGA-Net: 使用多目标遗传算法进行神经网络搜索”, 在过程中, 热内特, 进化, 电脑. Conf., 布拉格, 捷克共和国, 2019 年 7 月, 第 419-427 页。
- [28] J. Jiang, F. Han, Q. Ling, J. Wang, T. Li 和 H. Han, “通过基于分解的多目标粒子群优化进行高效网络架构搜索”, 神经网络, 卷. 123, 第 305-316 页, 2020 年 3 月。
- [29] E. Real, A. Aggarwal, Y. Huang 和 QV Le, “图像分类器架构搜索的正则化演化”, Proc. AAAI 会议, 神器, 情报, 2019, vol. 33, 没有. 1, 页. 4780-4789。
- [30] Z. Lu, K. Deb, E. Goodman, B. Wolfgang 和 NB Vishnu, “NSGANetV2: 进化多目标代理辅助神经网络搜索”, Proc. 欧元. 会议, 电脑, 可见. (ECCV), 英国格拉斯哥, 纽卡斯尔大学, 2020, p. 3.
- [31] E. Real, S. Moore, A. Selle, S. Saxena, YL Suematsu, J. Tan, QV Le 和 A. Kurakin, “图像分类器的大规模演化”, 载于 Proc. 第 34 国际会议, 马赫. Learn., 澳大利亚新南威尔士州悉尼, 2017 年, 第 2902-2911 页。
- [32] L. Xie 和 A. Yuille, Proc 中的 “Genetic CNN”。IEEE 译释, 会议, 电脑, 可见. (ICCV), 威尼斯, 意大利, 10 月 2017 年, 第 101-1 页 1388-1397。
- [33] FE Fernandes Junior 和 GG Yen, “用于图像分类的深度神经网络架构的粒子群优化”, Swarm Evol. 计算机, 卷. 49, 第 62-74 页, 2019 年 9 月。
- [34] X. He, K. Zhao 和 X. Chu, “AutoML: 最先进技术的调查”, 2019 年, arXiv:1908.00709. [在线的]. 可用 <http://arxiv.org/abs/1908.00709> [35] R. Elshaw, M. Maher 和 S. Sakr, “自动化机器学习: 最先进的和开放的挑战”, 2019 年, arXiv:1906.02287. [在线的]. 可用 <http://arxiv.org/abs/1906.02287>
- [36] N. Ma, X. Zhang, HT Zheng 和 S. Jian, “ShuffleNet V2: 高效 CNN 架构设计实用指南”, Proc. 欧元. 会议, 帐户你要. (ECCV), 慕尼黑, 德国, 2018 年, pp. 116-131。
- [37] P. Molchanov, S. Tyree, T. Karras, A. Timo 和 K. Jan, “修剪卷积神经网络以实现资源高效推理”, 载于 Proc. 5 译释, 会议, 学习, 代表. (ICLR), 法国土伦, 2017 年, 第 1-17 页。
- [38] Y. Shu, W. Wang 和 S. Cai, “了解通过基于细胞的神经架构搜索学习的架构”, Proc. 译释, 会议, 学习, 代表. (ICLR), 亚的斯亚贝巴, 埃塞俄比亚, 2020 年, 第 101-1 页 21-21。
- [39] B. Zoph, V. Vasudevan, J. Shlens 和 QV Le, “学习可扩展图像识别的可迁移架构”, Proc. IEEE/CVF 会议, 计算, 可见. Pattern Recognit., 美国犹他州盐湖城, 6 月. 2018 年, 第 101-1 页 1-14。
- [40] Z. Zhong, J. Yan, W. Wu, J. Shao 和 C.-L. Liu, Proc 中的 “实用块智能神经网络架构生成”。IEEE/CVF 会议, 计算, 可见. Pattern Recognit., 美国犹他州盐湖城, 6 月. 2018 年, 第 101-1 页 2423-2432。
- [41] A. Krizhevsky, I. Sutskever 和 GE Hinton, “使用深度卷积神经网络的 ImageNet 分类”, Commun. 美国计算机学会, 卷. 60, 没有. 6, 第 84-90 页, 2017 年 5 月。
- [42] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke 和 A. Rabinovich, “深入卷积”, 载于过程. IEEE 会议, 电脑, 可见. 模式识别. (CVPR), 美国马萨诸塞州波士顿, 2015 年 6 月, 第 1-9 页。
- [43] LM Herstein, YR Filion 和 KR Hall, “使用基于 EIO-LCA 的多目标优化评估配水系统的环境影响”, J. Water Resour. 规划管理, 卷. 137, 没有. 2, 第 162-172 页, 2011 年 3 月。
- [44] C. Li, X. Yuan, C. Lin, M. Guo, W. Wu, J. Yan 和 W. Ouyang, “AM-LFS: 用于损失函数搜索的 AutoML”, Proc. IEEE/CVF 译释, 会议, 电脑, 可见. (ICCV), 韩国首尔, 10 月 2019 年, 第 101-1 页 8409-8418。
- [45] Y. He, J. Lin, Z. Liu, H. Wang, L.-J. Li 和 S. Han, “AMC: 用于移动设备上的模型压缩和加速的 AutoML”, Proc. 欧元. 计算机设置可见. (ECCV), 2018 年 9 月, 第一卷. 112, 没有. 第 11 页 815-832。
- [46] B. Zoph 和 QV Le, “使用强化学习进行神经架构搜索”, Proc. 译释, 会议, 学习, 代表. (ICLR), 法国土伦: Palais des Congrès Neptune, 2017 年, 第 1-16 页。
- [47] G. Bender, H. Liu, B. Chen, G. Chu, S. Cheng, P.-J. Kindermans 和 QV Le, “权重共享能否优于随机架构搜索? Proc. 中的 TuNAS 调查. IEEE/CVF 会议, 计算, 可见. 模式识别. (CVPR), 美国华盛顿州西雅图, 2020 年 6 月, 第 14311-14320 页。
- [48] D. Kwon, K. Natarajan, SC Suh, H. Kim 和 J. Kim, “使用卷积神经网络进行网络异常检测的实证研究”, Proc. IEEE 第 38 届国际会议, 会议, 分发, 电脑, 系统. (ICDCS), 奥地利维也纳, 2018 年 7 月, 第 1595-1598 页。
- [49] X. Yuan, C. Li 和 X. Li, “DeepDefense: 通过深度学习识别 DDoS 攻击”, Proc. IEEE 译释, 会议, 智能电脑. (SMARTCOMP), 香港, 2017 年 5 月, 第 1-8 页。
- [50] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del-Rincon 和 D. Siracusa, “Lucid: 用于 DDoS 攻击检测的实用、轻量级深度学习解决方案”, IEEE 跨, 网络, 服务管理, 卷. 17, 没有. 2, 第 876-889 页, 2020 年 6 月。
- [51] J. Mei, Y. Li, X. Lian, XJ Jin 和 LJ Yang, “AtomNAS: 细粒度端到端神经架构搜索”, Proc. 译释, 会议, 学习, 代表. (ICLR), 亚的斯亚贝巴, 埃塞俄比亚, 2020 年, 第 101-1 页 1-14。
- [52] DH Song, C. Xu, X. Jia 和 YY Chen, “ESR-EA: 图像超分辨率的高效残差密集块搜索”, Proc. AAAI 会议, 神器, 英特尔, 2020 年, 第一卷 34, 没有. 第 7 页 12007-12014。
- [53] LW Yao, H. Xu, W. Zhang, XD Liang 和 ZG Li, “SM-NAS: 用于对象检测的结构到模块化神经架构搜索”, Proc. AAAI 会议, 神器, 情报, 2020, 卷. 34, 没有. 7, 第 12661-12668 页。
- [54] C. Jiang, H. Xu, W. Zhang, X. Liang 和 Z. Li, “SP-NAS: 对象检测的串行到并行主干搜索”, Proc. IEEE/CVF 会议, 帐户你要, 模式识别. (CVPR), 君. 2020, 页. 11860-11869。
- [55] A. Abayomi-Alli, S. Misra, L. Fernández-Sanz, O. Abayomi-Alli 和 AR Edun, 自动贩卖机, 软计算, 卷. 26, 没有. 3, 第 385-396 页, 2020 年。
- [56] PK Ray, S. Nandkeolyar, CS Lim 和 INW Satiawan, “使用非支配排序遗传算法 II 的需求响应管理”, Proc. IEEE 译释, 会议, 电力电子, 智能电网更新, 能源 (PESGRE), 印度科钦, 2020 年 1 月, 第 1-6 页。
- [57] H. Chen 和 S. Kuo, “基于熵测量的主动检测 DDOS 攻击方法用于智能手机上的下一代即时消息应用程序”, Intell. 自动贩卖机, 软计算, 卷. 25, 没有. 1, 第 217-228 页, 2019 年。
- [58] L. Shen, X. Chen, Z. Pan, K. Fan, F. Li 和 J. Lei, “基于全局和局部内容特征的无参考立体图像质量评估”, 神经计算, 卷. 424, 第 132-142 页, 2021 年 2 月, doi: 10.1016/j.neucom.2020.10.024。
- [59] Z. Pan, X. Yi, Y. Zhang, B. Jeon 和 S. Kwong, “基于增强型深度卷积神经网络的 HEVC 高效环内滤波”, IEEE Trans. 图像处理, 卷. 29, 第 5352-5366 页, 2020 年。
- [60] Z. Pan, X. Yi, Y. Zhang, H. Yuan, FL Wang 和 S. Kwong, “基于 HEVC 视频内容特征的帧级位分配优化”, ACM Trans. 多媒体计算机, Commun. Appl., 卷. 16, 没有. 1, 第 1-20 页, 2020 年。
- [61] E. Zitzler, M. Laumanns 和 L. Thiele, “SPEA2: 提高帕累托进化算法的强度”, Proc. 进化, 方法设计优化, 控制应用程序, 工业问题, 2001 年, 第 95-100 页。
- [62] CAC Coello 和 MS Lechuga, “MOPSO: 多目标粒子群优化建议”, Proc. 国会进化, Comput., 檀香山, HI, 美国, 2002 年 12 月, 第 1051-1056 页。
- [63] K. Deb, A. Pratap, S. Agarwal 和 T. Meyarivan, “一种快速的精英多目标遗传算法: NSGA-II”, IEEE Trans. 进化, 计算机, 卷. 6, 没有. 2, 第 182-197 页, 2002 年 4 月。
- [64] K. Deb 和 H. Jain, “使用基于参考点的非支配排序方法的进化多目标优化算法, 第一部分: 解决框约束问题”, IEEE Trans. 进化, 计算机, 卷. 18, 没有. 4, 第 577-601 页, 2014 年 8 月。
- [65] Q. Zhang 和 H. Li, “MOEA/D: 基于分解的多目标进化算法”, IEEE Trans. 进化, 计算机, 卷. 11, 没有. 6, 第 712-731 页, 2007 年 12 月。
- [66] T. Pamulapati, R. Mallipeddi 和 PN Suganthan, “ISDE+ 多目标优化指标”, IEEE Trans. 进化, 计算机, 卷. 23, 没有. 2, 第 346-352 页, 2019 年 4 月。
- [67] Z. Li, X. Wang, S. Ruan, Z. Li, C. Shen 和 Y. Zeng, “基于改进的超体积的多目标高效全局优化方法的预期改进”, Struct. 多学科优化, 卷. 58, 没有. 5, pp. 1961-1979, 2018 年 11 月。
- [68] Y. Sun, GG Yen 和 Z. Yi, “用于多目标优化问题的基于 IGD 指标的进化算法”, IEEE Trans. 进化, 计算机, 卷. 23, 没有. 2, 第 173-187 页, 2019 年 4 月。
- [69] X. He, X. Fu 和 Y. Yang, “基于多目标 PSO 的无线传感器网络移动接收器的节能轨迹规划算法”, IEEE Access, 卷. 7, 第 176204-176217 页, 2019 年。
- [70] H. Mofid, H. Jazayeri-Rad, M. Shahbazian 和 A. Fetanat, “使用多目标粒子群优化 (MOPSO) 算法提高并行氮气膨胀液化过程 (NELP) 的性能”, 能源, 卷. 172, 第 286-303 页, 2019 年 4 月。

[71] S. Khalid, A. Ishfaq and K. Mohammad E., “在智能电网环境中优化数据中心利润的进化方法”, Proc. 第二诠释。会议。数据英特尔。安全的。(ICDIS), 南帕诸岛, 德克萨斯州, 美国, 6月。2019, 页。89–96。

[72] M. Ohki, “NSGA-II 的有效性 & 线性安排的 Pareto-partial 优势对于实用的多目标护士安排”, 在 Proc. 第七诠释。会议。控制。决定。信息。技术。(CoDIT), 布拉格, 捷克共和国, 2020年6月, 第 581–586 页。



RENJIAN LV 获得北京航空航天大学软件工程学士学位。他目前正在攻读博士学位。北京邮电大学信息安全专业毕业。2006年至今在华北计算技术研究院工作,任工程师,研究室主任。他在与无线网络、嵌入式系统、信息安全和物联网等 ICT 技术相关的技术和产业发展研究方面拥有早 15 年的经验。他是欧盟-中国物联网咨询小组的初级专家,也是 ISO/IEC JTC1/WG10 的专家。



王晓娟获得博士学位。北京邮电大学电子科学与技术专业毕业。现任北京邮电大学电子工程学院副教授。她的研究兴趣包括深度学习、复杂网络和人体手势识别。



BINGYING DAI 2017 年于厦门大学获得统计学硕士学位,目前在读博士。科罗拉多州立大学统计学学位。她的研究兴趣包括网络分析和机器学习。



XINLEI WANG 于 2019 年获得中国山东省山东科技大学通信工程学士学位。她目前正在攻读硕士学位。北京邮电大学本科, 中国北京。

她的研究兴趣包括深度学习和计算机网络安全。



MINGSHU HE 于 2017 年在中国北京的北京邮电大学获得工学学士学位,目前正在攻读博士学位。程度。他的研究兴趣包括网络安全、异常检测和机器学习。



雷进获得博士学位。他于 2015 年在中国北京的北京邮电大学获得博士学位,目前正在攻读博士学位。程度。他的研究兴趣包括复杂网络和深度学习。



吕天琪于 2015 年获得河北燕山大学电子信息工程学士学位,目前正在攻读博士学位。北京邮电大学本科, 中国北京。

他的研究兴趣包括深度学习和人工智能。

...