Modeling and Simulation 建模与仿真, 2025, 14(5), 579-590
Published Online May 2025 in Hans. https://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2025.145416

Hans汉斯

基于半监督学习的加密流量分类模型CLGAN

邸　展[1]，刘　亚[1,2]，赵逢禹[3]，曲　博[4]

[1]上海理工大学光电信息与计算机工程学院，上海
[2]香港狮子山网络安全实验室，香港
[3]上海出版印刷高等专科学校信息与智能工程系，上海
[4]港专学院网络空间科技学院，香港

收稿日期：2025年4月20日；录用日期：2025年5月13日；发布日期：2025年5月20日

摘　要

加密流量的快速增长和复杂化对网络流量分类提出了新的挑战。针对现有方法在加密流量分类中特征提取能力不足和标注数据需求量大的问题，文章提出了一种基于生成对抗网络(GAN)的半监督加密流量分类模型CLGAN。通过对GAN网络中的判别器使用CNN与LSTM级联结构，模型能够有效结合卷积神经网络(CNN)的空间特征提取能力与长短时记忆网络(LSTM)的时序特征捕获能力，从而提升分类性能。在公开数据集ISCX2012 VPN-nonVPN和USTC-TFC2016上，分别与半监督学习模型DCGAN、基于AE的半监督学习模型以及监督学习模型CNN-LSTM进行对比实验。实验结果表明：CLGAN在标注数据稀缺场景下表现出更强的特征提取和泛化能力。当标记样本数量为2000时，CLGAN的分类准确率比CNN-LSTM模型提高了约3%；与模型DCGAN相比，在不同数据标记数量下CLGAN模型分类准确率均提高了约4%。

关键词

加密流量分类，深度学习，半监督学习，注意力机制，生成对抗网络

Encrypted Traffic Classification Model CLGAN Based on Semi-Supervised Learning

Zhan Di[1], Ya Liu[1,2], Fengyu Zhao[3], Bo Qu[4]

[1]School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai
[2]Hong Kong Lion Rock Cyberspace Security Laboratory, Hong Kong
[3]Department of Information and Intelligent Engineering, Shanghai Publishing and Printing College, Shanghai
[4]Institute of Cyberspace Technology, Hong Kong College of Technology, Hong Kong

Received: Apr. 20th, 2025; accepted: May 13th, 2025; published: May 20th, 2025

文章引用: 邸展, 刘亚, 赵逢禹, 曲博. 基于半监督学习的加密流量分类模型CLGAN [J]. 建模与仿真, 2025, 14(5): 579-590.
DOI: 10.12677/mos.2025.145416

Abstract

The rapid growth and complexity of encrypted traffic pose new challenges to network traffic classification. Aiming at the problems of insufficient feature extraction ability and great demand for labeled data in existing methods for encrypted traffic classification, this paper proposes a semi-supervised encrypted traffic classification model CLGAN based on the Generative Adversarial Network (GAN). By using a cascade structure of Convolutional Neural Network (CNN) and Long Short-Term Memory network (LSTM) in the discriminator of the GAN network, the model can effectively combine the spatial feature extraction ability of the CNN and the temporal feature capture ability of the LSTM, thus improving the classification performance. Comparative experiments are conducted on the public datasets ISCX2012 VPN-nonVPN and USTC-TFC2016, comparing with the semi-supervised learning model DCGAN, the semi-supervised learning model based on Autoencoder (AE), and the supervised learning model CNN-LSTM. The experimental results show that CLGAN exhibits stronger feature extraction and generalization capabilities in scenarios where labeled data is scarce. When the number of labeled samples is 2000, the classification accuracy of CLGAN is approximately 3% higher than that of the CNN-LSTM model; compared with the DCGAN model, the classification accuracy of the CLGAN model is approximately 4% higher under different numbers of labeled data.

Keywords

Encrypted Traffic Classification, Deep Learning, Semi-Supervised Learning, Attention Mechanism, Generative Adversarial Network

1. 引言

随着通信网络的快速发展，网络流量数据的类型和数量也相应地不断增加。网络流量分类已成为网络管理与安全领域中一项重要的研究任务。它无疑是动态访问控制、网络资源调度、服务质量(QoS)保障、入侵和恶意软件检测等方面的基石。高效且准确的流量分类对于提供服务质量保障、动态访问控制以及检测异常网络行为具有重大的现实意义。然而，随着包括 5G 和物联网在内的网络中加密技术的广泛应用，部分加密流量的增长给诸如服务质量保障之类的网络管理工作带来了巨大挑战。因此，准确且可靠的加密流量分类不仅有助于改善细粒度的网络资源分配，还能实现策略驱动的网络管理。

目前已有一些使用流量统计信息进行加密流量分类的流量分类器，它们能够取得不错的性能，但其需要领域专家手工设计特征，这往往非常耗费精力。而生成对抗网络(GAN)在内的深度学习(DL)技术能够在无需人工干预的情况下自动提取特征，这无疑使其成为流量分类，尤其是加密流量分类中非常理想的方法。近期的研究工作已经证明了深度学习方法在流量分类方面的优越性[1]，例如多层感知机(MLP) [2]、卷积神经网络(CNN) [3]-[7]、栈式自编码器(SAE) [8]、长短期记忆网络(LSTM) [9] [10]等。

基于深度学习的加密流量分类研究工作大多需要大量的标注数据集，也就是监督学习，这一直是深度学习领域大多数研究的核心。目前流量数据集主要有两种标注方法，一种是基于深度包检测(DPI)的标注方法，另一种是基于脚本的标注方法。然而，基于深度包检测的标注方法无法处理加密流量，而基于脚本的方法也并不总是准确的。且获取大量标注数据集是一项繁琐且耗时的手工劳动，未标注数据总是

丰富且容易获取的。因此，开发能够从较少量数据中学习的模型的需求日益迫切，半监督学习是克服这一问题的合适技术。Wang 等[11]进一步优化了 GAN 模型，提出了一种基于半监督生成对抗网络的流量分类方法——ByteSGAN，特别适用于 SDN 边缘网关中的加密流量分类任务，该方法利用 GAN 的生成对抗机制和基于字节流的特征表示，从而在标签稀缺的情况下显著提升分类性能。变分自动编码器作为另一种生成模型，通过学习未标注数据的潜在特征分布，为半监督学习模型提供了更丰富的特征表示。

本文提出了一个半监督学习模型——CLGAN (CNN and LSTM Generative Adversarial Networks)，该模型巧妙地结合了 GAN 生成器产生的样本和未标记数据，通过改进 GAN 鉴别器网络的结构，实现了在少量标记样本上的高效学习。这种半监督学习策略不仅显著降低了对大规模标注数据的依赖，还提高了分类器的性能，为网络流量分类提供了一种更为经济和实用的解决方案。基于公开数据集 ISCX2012 VPN-non VPN 和 USTC-TFC2016 的实验结果表明，CLGAN 在标注数据稀缺场景下表现出更强的特征提取和泛化能力。当标记样本数量为 2000 时，CLGAN 的分类准确率比 CNN-LSTM 模型提高了约 3%；与模型 DCGAN 相比，在不同数据标记数量下 CLGAN 模型分类准确率均提高了约 4%。

2. 网络模型架构

本节将深入探讨基于生成对抗网络的半监督加密流量分类模型的设计内容。

2.1. 网络模型整体概述

为实现基于无标签数据集的加密流量分类目标，本文提出了一种基于生成对抗网络的半监督分类模型 CLGAN，其整体架构如图 1 所示。该模型由生成器 G 和鉴别器 D 两部分组成。通过对传统 GAN 的改进，生成器 G 中使用卷积神经网络(CNN)，利用反卷积技术生成模拟加密流量数据。这些模拟数据与未标记的真实加密流量数据共同用于训练鉴别器 D，使其能够在交叉训练过程中学习加密流量的特征。此外，鉴别器 D 的结构被优化为 LSTM 与 CNN 的级联网络，以增强对加密流量的时空特征提取能力，从而更全面地捕捉深层信息。最终，提取的特征张量通过 Softmax 分类器完成加密流量的分类任务。

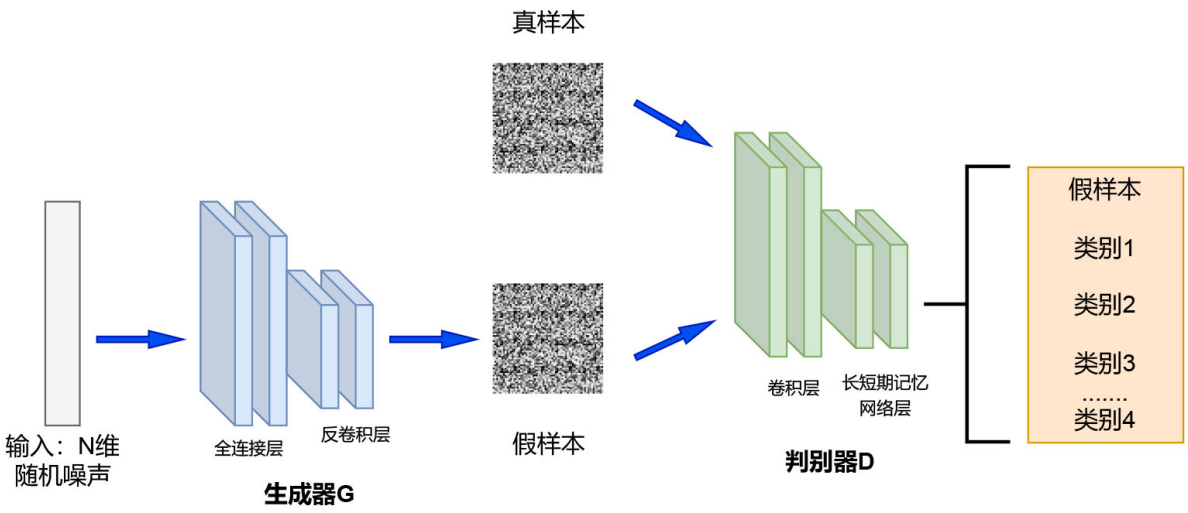

Figure 1. The network architecture of CLGAN
图 1. CLGAN 网络模型结构

CLGAN 继承了 DCGAN 生成器的基本框架，包括转置卷积上采样、批归一化等核心组件，保持了 GAN 对抗训练的基本范式。关键区别在于判别器架构的革新：DCGAN 采用纯 CNN 判别器，主要提取

空间局部特征，而 CLGAN 创新性地将 CNN 与 LSTM 结合，形成混合判别器架构。这种设计使 CLGAN 能同时捕捉流量的空间特征(通过 CNN)和时序动态特性(通过双向 LSTM)，特别是通过时空特征交叉注意力融合机制，有效解决了传统 DCGAN 在处理流量数据时难以建模长程时序依赖的问题。

在 CLGAN 模型中，左侧蓝色部分为生成器 G，其生成的模拟加密流量数据与真实加密流量数据(如中间黑色框图所示)共同作为鉴别器 D 的输入，通过反向传播完成 D 的训练。模型的训练过程与传统 GAN 类似，生成器 G 和鉴别器 D 通过交叉训练进行极大极小博弈，使生成器 G 能够生成接近真实流量分布的数据，同时鉴别器 D 在训练过程中学习加密流量的时空特征。随后，将鉴别器 D 的权重迁移至新的分类器，并利用带标签数据进行微调，最终完成加密流量的分类任务。这一过程体现了 CLGAN 实现半监督加密流量分类的核心原理。

2.2. 鉴别器结构

在加密流量分类研究中，时序特征学习通常采用基于流或基于会话(即双向流)两种方式。根据文献[4]的研究，基于流的方法在分类效果上更具优势。因此，本文利用 CNN 和 LSTM 的结合，以基于会话的方式学习时序特征。首先，通过 CNN 提取流量的空间特征，生成特征张量。随后，将特征张量输入到 LSTM 中，进一步提取时序特征，最终得到加密流量的时空特征。为防止过拟合，网络在输出前加入了 Dropout 层[12]，并将特征张量输入 Softmax 分类器，得到鉴别器的分类结果。

图 2 展示了 CLGAN 模型中鉴别器 D 的网络结构。鉴别器 D 的输入包括生成器 G 生成的模拟加密流量数据和真实流量数据。其中，CNN 用于提取空间特征，LSTM 则用于提取时序特征，两者共同完成加密流量的特征学习任务。

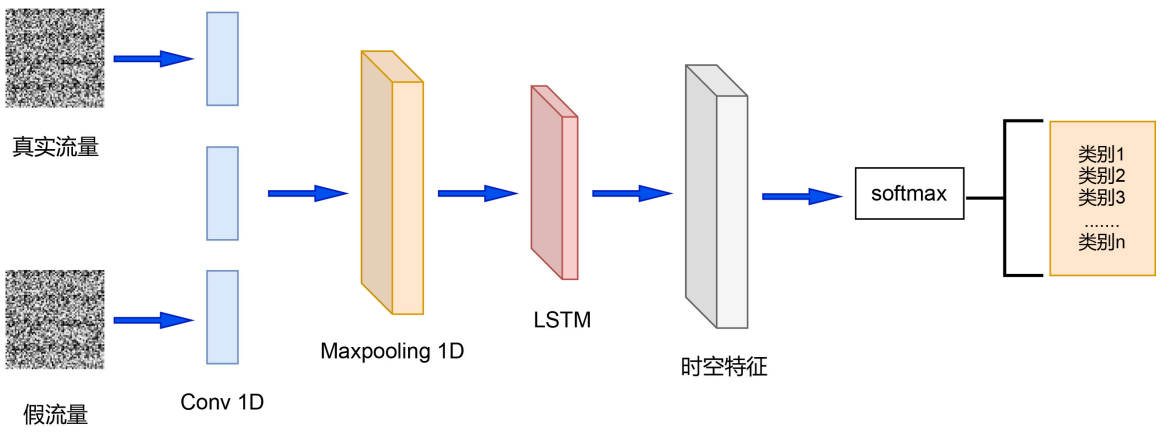

Figure 2. Discriminator D architecture in CLGAN
图 2. CLGAN 模型中鉴别器 D 的结构图

鉴别器采用 CNN 与 LSTM 结合的深度判别模型，用于对 28 × 28 的流量数据进行分类。该模型由两个一维卷积层和一个 LSTM 层构成。首先，第一个一维卷积层以 28 × 28 的流量数据为输入，输出 128 维特征序列，卷积核大小为 5，步长为 1，填充为 2。第二个一维卷积层以 128 维特征序列为输入，输出 64 维特征序列，卷积核大小同样为 5，步长为 1，填充为 2。接着，将 64 维特征序列输入 LSTM 层，提取时序特征，输出 256 维特征序列。最终，通过全连接层将时空特征映射到 12 个类别中，并通过 Softmax 层输出分类结果。

在加密流量分类研究中，Iliyasu 团队[13]构建的 DCGAN 半监督模型虽取得良好效果，但其鉴别器 D

的单 CNN 结构难以有效捕捉时序特征。本研究针对该局限性进行改进，提出时空特征融合分类网络：将鉴别器的 CNN 模块替换为 CNN 与 LSTM 的级联架构。通过采用“CNN→LSTM”的特征处理顺序，在优先提取流量数据空间依赖的基础上，再利用 LSTM 捕获局部时序特征，从而避免传统“LSTM→CNN”结构中卷积操作对空间连续性的破坏。实验表明，这种级联方式显著提升了加密流量的时空特征表征能力，最终实现分类性能的优化。

2.3. 生成器结构

生成器 G 如图 3 所示。由全连接层、重塑层、多级反卷积层和时序特征增强模块构成。具体如下：

全连接层：首先，输入的 100 维噪声向量通过全连接层进行线性变换，输入维度为 100，输出维度为 2048，以适配后续反卷积层的多级扩展需求。这进一步将噪声向量映射到更高维空间，为特征生成提供基础。

重塑层：全连接层的输出被展平成一个长度为 2048 的向量。这个向量被重塑为一个形状为(128 × 4 × 4)的特征图。128 表示特征图通道数，4 × 4 表示特征图的高度和宽度。

反卷积层：反卷积层都使用大小为 5 × 5 的卷积核，步长为 2，填充为 1。第一级反卷积，输入为 128 通道的 4 × 4 特征图，输出尺寸为 64 × 8 × 8，选用 LeakyReLuck 激活函数增强梯度传播稳定性。第二层反卷积，输入为 64 通道的 8 × 8 特征图，输出尺寸为 32 × 16 × 16，同样使用 LeakyReLuck 激活函数。第三层反卷积层的输入为 32 通道的 16 × 16 特征图，最后输出尺寸为 1 × 28 ×28，确保与鉴别器的输入尺寸一致，最后选用 Tanh 激活函数。在每级反卷积后加入 Batch Normalization 层，以此来加速训练收敛并提升生成稳定性。生成的模拟流量数据与真实流量数据一起作为鉴别器 D 的输入。

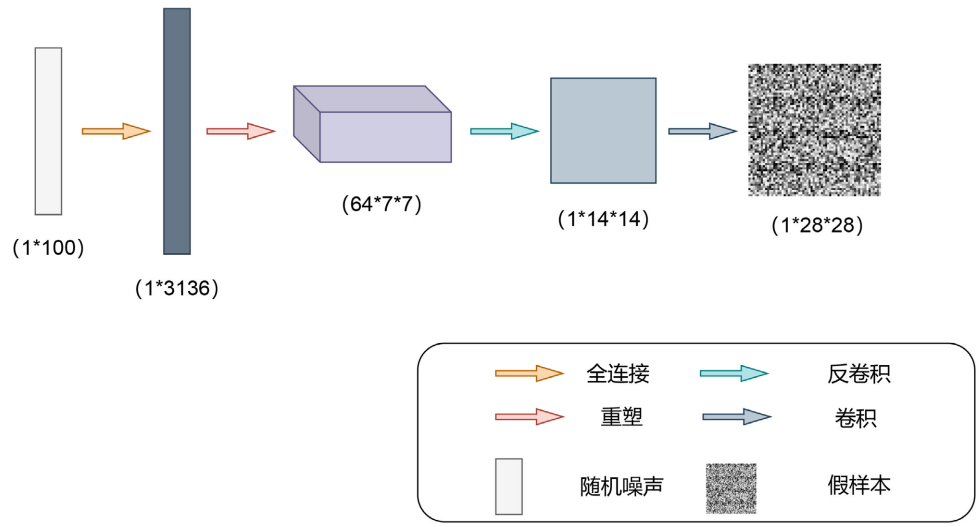

Figure 3. Generator G architecture in CLGAN
图 3. CLGAN 模型中生成器 G 的结构图

2.4. 网络训练过程

CLGAN 网络的输入为无标签数据集 *Sul*、带标签数据集 *Sl*；输出为鉴别器 D 输出的流量分类结果。半监督训练流程分为三个阶段：无监督预训练、参数微调和流量分类，具体步骤如下：

无监督预训练阶段：将混合数据集 *Sul* 和 *Sl* 输入网络，通过生成器 G 与鉴别器 D 的交替训练，促使两者在对抗博弈中达到动态平衡。在此过程中，生成器 G 通过模拟流量生成辅助鉴别器 D 学习加密流量

的时空特征分布，同时保存两者的权重参数。

参数迁移与监督微调：加载预训练的鉴别器 D 权重，基于带标签数据集*Sl*进行全监督微调，优化分类边界并提升模型对标记数据的适配性。

流量分类：将待分类流量数据输入微调后的鉴别器 D，通过特征提取与 Softmax 分类输出最终类别概率。

该算法通过预训练阶段利用无标签数据增强特征学习能力，再结合少量标签数据细化分类性能，有效缓解数据标注不足的瓶颈问题。

3. 实验分析

为全面验证 CLGAN 方案的优势，本文选取两个国际公开数据集，即 ISCX VPN-nonVPN 和 USTC-TFC2016，对该模型性能展开测试。同时，与多个半监督学习模型及监督学习模型进行对比试验。实验结果清晰地表明，CLGAN 在性能方面展现出显著的优越性。

3.1. 损失函数

图 4 展示了 CLGAN 模型在训练过程中的损失函数收敛曲线，其中橙色曲线表示生成器的损失，蓝色曲线表示判别器的损失。从图中可以观察到以下几个关键特征：在训练的初始阶段，生成器的损失迅速下降，而判别器的损失逐步上升。这一现象表明，随着生成器不断优化，其生成的样本质量逐渐提高，从而使判别器更难以区分真实样本和生成样本。随着训练的进行，生成器和判别器的损失逐渐趋于平稳，分别在较低的波动范围内维持。此时，生成器与判别器达到了动态平衡，表明 CLGAN 模型进入了稳定的对抗训练阶段。从损失曲线的变化可以看出，生成器和判别器之间保持了良好的对抗关系。生成器的损失稳定后保持在较高水平，而判别器的损失保持在较低水平，表明生成器能够生成较为逼真的样本，同时判别器能够对样本进行有效的分类。

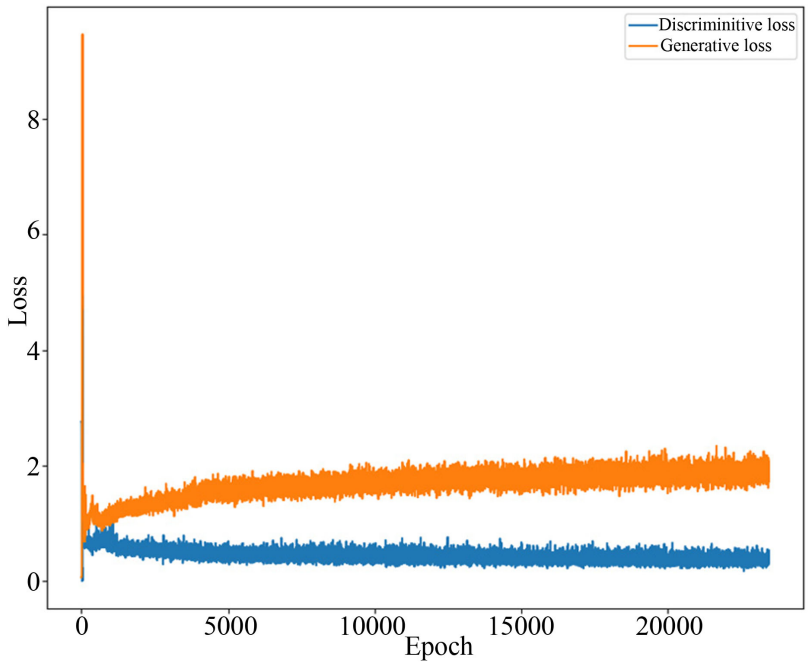

Figure 4. The training loss function of CLGAN
图 4. CLGAN 训练损失函数

3.2. 与半监督学习实验对比

本研究以 DCGAN 半监督分类模型为基础架构，针对其鉴别器模块进行了优化改进。从而克服了原始模型仅能提取空间特征的局限性，实现了对加密流量时空特征的综合提取。基于这一改进思路构建了 CLGAN 模型，因此实验环节选择 DCGAN 作为基准对比网络，以验证模型改进的有效性。本实验基于前文所述的模型架构展开，选用 ISCX VPN-nonVPN 数据集进行验证。为考察不同标注数据量的影响，实验设置了 10%、30%、50%、70%四个标注比例等级。性能评估采用分类准确率(Accuracy)指标，具体实验结果详见表 1。

Table 1. Classification accuracy comparison with DCGAN
表 1. 与 DCGAN 模型分类精度对比

Labeled	CLGAN	DCGAN
10%	94.22	89.27
30%	96.85	91.36
50%	98.56	93.20
70%	98.97	94.17

实验结果表明，在不同标注比例条件下，本文提出的 CLGAN 模型均展现出最优的分类性能。具体而言，当标注数据比例为 10%、30%、50%和 70%时，模型分类准确率分别达到 94.22、96.85、98.56 和 98.97。与基准模型 DCGAN 相比，CLGAN 在四种数据配置下均实现了约 4%的性能提升，这主要得益于模型鉴别器中引入的时序特征提取机制，通过 CNN-LSTM 混合架构有效捕获了加密流量的时空特征，从而显著提升了分类性能。

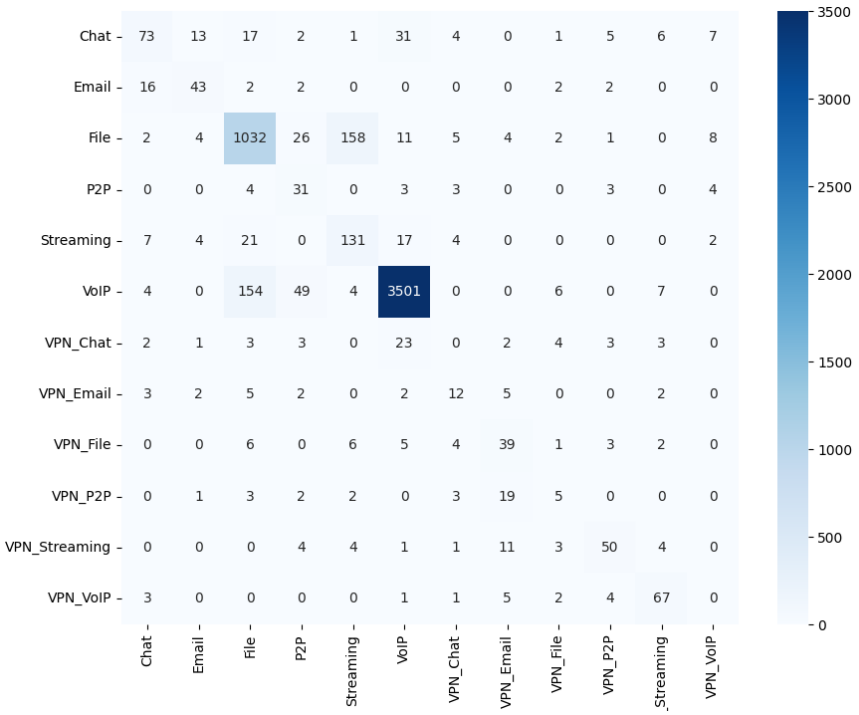

Figure 5. Confusion matrix of the CLGAN classification
图 5. 基于 CLGAN 分类的混肴矩阵

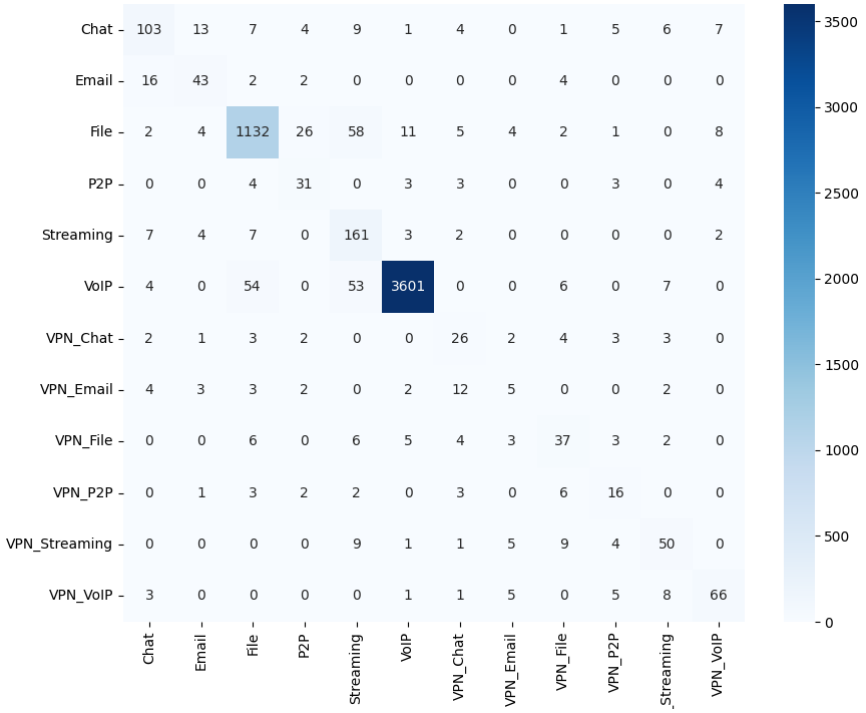

Figure 6. Confusion matrix of the DCGAN classification
图 6. 基于 DCGAN 的分类混肴矩阵

与 DCGAN 相比 CLGAN 方案提出时空特征融合分类网络，即将鉴别器采用 CNN 与 LSTM 的级联组合架构，通过采用“CNN→LSTM”的特征处理顺序，在优先提取流量数据空间依赖的基础上，再利用 LSTM 捕获局部时序特征，从而避免传统“LSTM→CNN”结构中卷积操作对空间连续性的破坏。这种级联方式提升了加密流量的时空特征表征能力，最终实现分类性能的优化。

前文已详细分析了半监督分类模型的准确率指标，本节将进一步展示 CLGAN 与 DCGAN 在 12 类加密流量分类任务中的混淆矩阵。图 5 和图 6 分别呈现了两个模型的分类效果对比。通过混肴矩阵能够看出 CLGAN 的分类效果要好于 DCGAN，这表明了该研究针对 DCGAN 提出的改进是有效的。

为了进一步验证 CLGAN 性能的优异性，本文设计并实现了一个基于自动编码器(AE)的半监督分类模型[14]。该模型包含两个部分：自动编码器和分类模型。自动编码器由两个主要组件构成，即编码器和解码器。编码器用作特征提取器，随着数据进入更深层次，它从低层次到高层次检测特征。提取的特征存储在潜在向量中。解码器获取这些特征并将它们转换回原始形状，输入流量数据，并尝试重构原始流量。分类器接收来自编码器的特征进行分类。自动编码器是一种无监督学习模型，将其与分类器相结合，形成一个半监督学习模型。具体模型结构如下：

输入层：数据采用 28 × 28 的灰度图。

编码器：使用一个三层的卷积神经网络(CNN)。每一层都有一个形状为(3, 3)的卷积核。编码器接收数据包字节向量(PBV)量，提取数据的空间特征，并将提取的特征存储在潜在向量中。

解码器：与生成式对抗网络(CLGAN)的生成器结构相同。

分类器：分类器由卷积神经网络(CNN)和长短时记忆网络(LSTM)结合构成。首先，CNN 模块作为特征提取器，利用两层卷积网络提取局部空间特征，每一层均采用形状为(3, 3)的卷积核。随后，提取的空间特征被传递到 LSTM 模块，进一步捕获特征的时序依赖关系，并强化对数据序列特性的学习。最终，LSTM 模块的输出通过全连接层，并使用 Softmax 激活函数输出分类结果。

在模型训练阶段，使用未标记的样本训练编码器和解码器，并将损失函数设置为平均绝对误差(MAE)。使用标记的样本训练编码器和分类器，并使用分类交叉熵作为损失函数。

如表 2 所示，可以发现两个模型都能利用少量有标签数据达到较高准确率。尽管差异不大，在相同标注数据量下，CLGAN 的所有指标均显著高于 AE。并且 CLGAN 的指标波动更小，而 AE 的波动范围更大，表明 CLGAN 对数据量的敏感性更低。从表 3 可以看出，在标注数据量较少时，如带标签数据量为 100 时，CLGAN 的准确率明显高于 AE。这表明 CLGAN 在半监督场景下具有更强的特征提取和泛化能力。当标注数据量提升至 1000 时，CLGAN 与 AE 的差距缩小，说明充足标注数据能部分弥补传统方法的劣势。无论是 CLGAN 还是 AE，标注数据量从 100 增加到 1000 时均显著提升性能。这表明标注数据对模型训练至关重要。CLGAN 在半监督学习框架下表现出色，尤其在标注数据稀缺时优势显著；而基于 AE 的半监督学习方法在标注数据充足时仍具竞争力。

Table 2. Classification accuracy on ISCX VPN-nonVPN dataset
表 2. 在 ISCX VPN-nonVPN 数据集上的分类准确性

	Labeled	Unlabeled	Accuracy	Precision	Recall	F1-score
CLGAN	1000	4000	97.8	97.5	97.8	97.5
	1000	6000	98.0	98.2	98.4	97.9
	1000	8000	98.1	98.1	98.4	98.1
AE	1000	4000	96.2	96.3	96.2	96.1
	1000	6000	96.5	96.2	96.4	96.4
	1000	8000	97.2	97.1	97.1	97.2

Table 3. Classification accuracy on USTC-TFC2016 dataset
表 3. 在 USTC-TFC2016 数据集上的分类准确性

	Labeled	Unlabeled	Accuracy	Precision	Recall	F1-score
CLGAN	100	4000	89.3	89.4	89.4	89.3
	100	8000	93.5	93.6	93.5	93.5
	100	12000	94.9	94.9	94.9	94.8
	1000	4000	98.0	98.3	98.1	98.5
	1000	8000	98.1	98.1	98.3	98.2
	1000	12000	98.6	98.6	98.6	98.7
AE	100	4000	83.2	83.7	83.7	83.9
	100	8000	90.3	90.1	90.3	90.2
	100	12000	93.0	93.0	93.1	92.9
	1000	4000	97.1	97.2	97.2	97.3
	1000	8000	98.0	97.2	97.2	97.2
	1000	12000	98.4	98.4	98.4	98.4

3.3. 与监督学习对比实验

本文选取的监督学习模型为 CNN 和 LSTM 的组合网络，在 ISCX VPN-nonVPN 数据集和 USTC-

TFC2016 数据集上分别对基于 CNN-LSTM 网络和基于 CLGAN 的分类模型开展实验。实验前，从数据集中选取指定数量的标记数据，其余作为未标记数据用于实验。采用随机梯度下降法进行训练，批量参数设为 256。噪声从区间[−1, 1]的均匀分布中随机采样，样本大小为 100。学习率参数设为 0.0002，并使用 Adam 优化器来优化生成器和判别器的损失函数。基于 CNN-LSTM 的加密流量分类模型由输入层、卷积层、池化层、LSTM 层和输出层组成。具体模型结构如下：

输入层：数据采用 28 × 28 的灰度图表示。

第一层卷积层：进行卷积操作，使用 128 个大小为 3、步长为 1 的滤波器。输出结果通过 ReLU 激活函数计算得出。

第一层池化层：采用最大池化，池化大小为 2，步长为 2。这样可以在减少数据量的同时保留重要特征。

第二层卷积层：使用 128 个大小为 3、步长为 1 的滤波器，输出结果通过 ReLU 激活函数计算得出。

第二层池化层：池化参数与第一层池化层相同，即池化大小为 2，步长为 2。

第三层卷积层：使用 128 个大小为 3、步长为 1 的滤波器，输出结果通过 ReLU 激活函数计算得出。

LSTM 层：卷积和池化操作后，将特征映射展开为时间序列输入到 LSTM 层。LSTM 层由 64 个单元组成，用于捕获流量特征的时序依赖关系。

全连接层：通过 LSTM 层的输出，将数据展平为一维向量，经过两个全连接层，用作后续分类。

输出层：使用 Softmax 分类法，输出层的神经元代表不同的应用程序。

在本文中，使用 CLGAN 在每类样本中分别只有 1000、2000、3000 和 4000 个标记数据的条件下进行分类实验，并将分类结果与相同条件下的 CNN-LSTM 模型进行对比，以证明 CLGAN 在半监督加密流量分类方面的优越性。

通过表 4 的实验结果可以看出，在 ISCX VPN-nonVPN 数据集上，当标记样本数量为 1000 时，CLGAN 的分类准确率比 CNN-LSTM 提高了约 4%。当标记样本数量为 2000 时，CLGAN 的分类准确率提高了约 3%。而当标记样本数量为 3000 时，CLGAN 的分类准确率提高幅度小于 1%。当标记样本数量为 4000 时，CLGAN 的分类准确率与 CNN-LSTM 相同。由此可见，当标记样本数量不足时，CLGAN 可以通过使用未标记样本以及 CLGAN 生成的样本来进行半监督学习，从而有效提高分类准确率。同样，通过表 5 能够发现，在标记样本数量较少时，CLGAN 的表现明显好于 CNN-LSTM，但随着标记样本数量的增加，两者之间的差距逐渐减小。

Table 4. Classification accuracy on ISCX VPN-nonVPN dataset
表 4. 在 ISCX VPN-nonVPN 数据集上的分类准确性

	Labeled	Accuracy	Precision	Recall	F1-score
CNN-LSTM	1000	88.5	88.8	88.4	88.6
	2000	89.8	89.9	89.8	89.7
	3000	92.7	92.4	92.6	92.5
	4000	93.6	93.7	93.6	93.6
CLGAN	1000	92.3	92.33	92.16	92.1
	2000	92.8	93.56	92.82	92.9
	3000	93.0	94.6	93.0	93.2
	4000	94.1	93.8	93.1	93.1

Table 5. Classification accuracy on USTC-TFC2016 dataset
表 5. 在 USTC-TFC2016 数据集上的分类准确性

	Labeled	Accuracy	Precision	Recall	F1-score
CNN-LSTM	1000	95.6	94.8	94.7	94.6
	2000	96.7	95.9	95.8	95.7
	3000	96.8	96.3	96.9	96.8
	4000	98.3	97.8	97.6	97.6
CLGAN	1000	98.2	98.1	98.1	96.0
	2000	98.5	98.2	98.8	97.9
	3000	98.8	98.8	98.9	98.2
	4000	98.9	98.9	99.1	99.1

4. 总结与展望

4.1. 总结

本文针对传统的网络流量分类方法在应对加密流量复杂性和标注数据稀缺性方面存在明显局限性这一问题，提出了一种基于生成对抗网络的半监督加密流量分类模型 CLGAN。本文的实验基于公开数据集 ISCX2012 VPN-nonVPN 和 USTC-TFC2016 展开，分别与经典的半监督学习模型，如 DCGAN 和基于 AE 的半监督学习模型以及监督学习模型 CNN-LSTM，进行了对比。实验结果表明，本文模型在标记样本数量较少的情况下，能够充分利用未标记数据集生成对抗框架中的生成样本，显著提升分类准确率，尤其在标记样本数量为 1000 和 2000 时，分类准确率较对比模型分别提高了约 4%和 3%。此外，随着标记样本数量的增加，本文模型与传统监督学习模型的性能差距逐渐缩小，验证了标记数据对分类任务的重要性。

4.2. 未来展望

尽管本研究取得了较好的实验结果，但仍存在一些值得进一步探讨的问题。当前模型在将 GAN 网络中的判别器改为 CNN 加 LSTM 结构后，显著增强了模型对时序和空间特征的捕获能力。但是模型的计算复杂度和训练时间需求仍然较高。未来可以探索以下优化方向：1) 利用轻量级神经网络，如 MobileNet 或 Tiny-LSTM，以降低模型复杂度，从而提高部署效率。2) 引入注意力机制(Attention Mechanism)，如 Transformer 或自注意力机制，进一步提升模型对关键特征的提取能力。3) 研究更高效的对抗训练策略，如通过改进生成器和判别器的损失函数，缓解 GAN 训练中不稳定的问题。

基金项目

本研究得到了国家自然科学基金资助项目(62002184)和香港狮子山网络安全实验室研究课题(LRL24017)的资助。

参考文献

[1] Aceto, G., Ciuonzo, D., Montieri, A. and Pescape, A. (2018) Mobile Encrypted Traffic Classification Using Deep Learning. 2018 *Network Traffic Measurement and Analysis Conference* (*TMA*), Vienna, 26-29 June 2018, 1-8. https://doi.org/10.23919/tma.2018.8506558

[2] Wang, P., Ye, F., Chen, X. and Qian, Y. (2018) Datanet: Deep Learning Based Encrypted Network Traffic Classification

in SDN Home Gateway. *IEEE Access*, **6**, 55380-55391. https://doi.org/10.1109/access.2018.2872430

[3] Lotfollahi, M., Siavoshani, M.J., Zade, R.S.H. and Saberian, M. (2017) Deep Packet: A Novel Approach for Encrypted Traffic Classification Using Deep Learning. *Soft Computing*, **24**, 1999-2012. http://www.arxiv.org https://doi.org/10.1007/s00500-019-04030-2

[4] Wang, W., Zhu, M., Wang, J., Zeng, X. and Yang, Z. (2017) End-to-End Encrypted Traffic Classification with One-Dimensional Convolution Neural Networks. 2017 *IEEE International Conference on Intelligence and Security Informatics* (*ISI*), Beijing, 22-24 July 2017, 43-48. https://doi.org/10.1109/isi.2017.8004872

[5] Wang, W., Zhu, M., Zeng, X., Ye, X. and Sheng, Y. (2017) Malware Traffic Classification Using Convolutional Neural Network for Representation Learning. 2017 *International Conference on Information Networking* (*ICOIN*), Da Nang, 11-13 January 2017, 712-717. https://doi.org/10.1109/icoin.2017.7899588

[6] Chen, Z., He, K., Li, J. and Geng, Y. (2017) Seq2Img: A Sequence-to-Image Based Approach Towards IP Traffic Classification Using Convolutional Neural Networks. 2017 *IEEE International Conference on Big Data* (*Big Data*), Boston, 11-14 December 2017, 1271-1276. https://doi.org/10.1109/bigdata.2017.8258054

[7] Chen, X., Yu, J., Ye, F. and Wang, P. (2018) A Hierarchical Approach to Encrypted Data Packet Classification in Smart Home Gateways. 2018 *IEEE* 16*th Intl Conf on Dependable, Autonomic and Secure Computing*, 16*th Intl Conf on Pervasive Intelligence and Computing*, 4*th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress* (*DASC/PiCom/DataCom/CyberSciTech*), Athens, 12-15 August 2018, 41-45. https://doi.org/10.1109/dasc/picom/datacom/cyberscitec.2018.00022

[8] Wang, Z. (2015) The Application of Deep Learning on Traffic Identification. http://www.blackhat.com

[9] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A. and Lloret, J. (2017) Network Traffic Classifier with Convolutional and Recurrent Neural Networks for Internet of Things. *IEEE Access*, **5**, 18042-18050. https://doi.org/10.1109/access.2017.2747560

[10] Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., *et al*. (2018) HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection. *IEEE Access*, **6**, 1792-1806. https://doi.org/10.1109/access.2017.2780250

[11] Wang, P., Wang, Z., Ye, F. and Chen, X. (2021) ByteSGAN: A Semi-Supervised Generative Adversarial Network for Encrypted Traffic Classification in SDN Edge Gateway. *Computer Networks*, **200**, Article 108535. https://doi.org/10.1016/j.comnet.2021.108535

[12] Srivastava, N., Hinton, G., Krizhevsky, A., *et al*. (2014) Dropout: A Simple Way to Prevent Neural Networks from Overfitting. *The Journal of Machine Learning Research*, **15**, 1929-1958.

[13] Iliyasu, A.S. and Deng, H. (2020) Semi-Supervised Encrypted Traffic Classification with Deep Convolutional Generative Adversarial Networks. *IEEE Access*, **8**, 118-126. https://doi.org/10.1109/access.2019.2962106

[14] Aouedi, O., Piamrat, K. and Bagadthey, D. (2020) A Semi-Supervised Stacked Autoencoder Approach for Network Traffic Classification. 2020 *IEEE* 28*th International Conference on Network Protocols* (*ICNP*), Madrid, 13-16 October 2020, 1-6. https://doi.org/10.1109/icnp49622.2020.9259390