2025 年 第 25 卷 第 18 期
2025, 25(18):07678-08
科 学 技 术 与 工 程
Science Technology and Engineering
ISSN 1671—1815
CN 11—4688/T

DOI:10.12404/j.issn.1671-1815.2405443
引用格式:王璇政, 徐志鹏, 李晓秋, 等. 边缘分布式深度学习工控协议的识别方法[J]. 科学技术与工程, 2025, 25(18): 7678-7685.
Wang Xuanzheng, Xu Zhipeng, Li Xiaoqiu, et al. Industrial control protocol recognition based on edge distributed deep learning[J]. Science Technology and Engineering, 2025, 25(18): 7678-7685.

# 边缘分布式深度学习工控协议的识别方法

王璇政[1], 徐志鹏[1], 李晓秋[1], 王海琛[1], 甘子奇[2], 沙哲一[2]
(1. 中海油安全技术服务有限公司, 天津 300456; 2. 天津大学智能与计算学部, 天津 300350)

**摘 要** 为解决工控行业中大量非标准协议带来的传统协议识别方法不适用性问题,通过基于边缘分布式深度学习的方法研究了工控协议识别技术。提出了一种基于卷积神经网络技术的工控协议识别方法:获取网络中真实工控协议数据并进行预处理,根据协议特性选择合适的卷积神经网络模型,隐式提取协议本质特征,实现对 7 种工控协议的识别分类,准确率可达 99.92%。此外,将工控协议识别模型部署至网络边缘,采用数据并行分布式策略,在边缘服务器计算集群中开展协同训练,模型训练效率提高 1.87~2.81 倍,同时保持高准确率。结果表明:该方法有效提高了工控协议识别准确率;显著提升了模型训练效率;适合部署于边缘计算环境。可见,该方法在工控协议识别性能优化方面具有重要意义。

**关键词** 工控协议识别; 深度学习; 卷积神经网络; 边缘智能; 分布式训练; 工业物联网
**中图法分类号** TP391.4; **文献标志码** A

# Industrial Control Protocol Recognition Based on Edge Distributed Deep Learning

WANG Xuan-zheng[1], XU Zhi-peng[1], LI Xiao-qiu[1], WANG Hai-chen[1], GAN Zi-qi[2], SHA Zhe-yi[2]
(1. CNOOC Safety Technology Service Co., Ltd., Tianjin 300456, China;
2. Department of Intelligence and Computing, Tianjin University, Tianjin 300350, China)

[**Abstract**] To address the limitations of traditional protocol recognition methods caused by the presence of numerous non-standard protocols in IC (industrial control) sector, a method based on edge-distributed deep learning was studied to enhance IC protocol recognition technology. A recognition method based on CNN (convolutional neural networks) was proposed: real IC protocol data from the network was collected and preprocessed, and an appropriate CNN model was selected according to protocol characteristics to implicitly extract the essential features of the protocols. This achieved classification and recognition of seven types of IC protocols with an accuracy of up to 99.92%. Furthermore, the IC protocol recognition model was deployed at the network edge, leveraging a data-parallel distributed strategy for collaborative training within an edge server computing cluster. This improved the training efficiency of the model by 1.87~2.81 times while maintaining high accuracy. The results show that this method significantly improves the accuracy of IC protocol recognition, greatly enhances model training efficiency, and is well-suited for deployment in edge computing environments. It is evident that this method has significant value in optimizing IC protocol recognition performance.

[**Keywords**] industrial control protocol identification; deep learning; convolutional neural network; edge intelligence; distributed training; industrial internet of things

随着德国工业 4.0、《中国制造 2025》的提出以及工业物联网的快速发展,信息技术和制造业的融合将整个工业系统带入了一个智能时代。传统的全封闭式工业控制系统信息安全风险遭受网络攻击的状况频繁发生。归根到底在于所制定的工控协议安全性较差。网络协议安全是工控系统信息安全的一项重要内容,如何识别和分析工控协议,是监控、保护和管理工控设备安全的基石和前提。

协议识别分类方法一般存在基于端口的识别分类、基于深度包检测的识别分类、基于行为模式的识别分类、基于机器学习(machine learning, ML)的识别分类四类方法。工控行业中的工控协议种类繁多,大多数是自定义的非标准协议,其结构也有别于传统的网络协议,在工控协议的识别中,需要对协议相关的报文数据进行特征提取,寻找标识协议的关键特征,从而进行协议的识别分类。特征

**收稿日期**: 2024-07-19 **修订日期**: 2025-03-21
**基金项目**: 河北省省级科技计划(22310301D)
**第一作者**: 王璇政(1986—),男,汉族,山东荣成人,硕士,高级工程师。研究方向:HSE 咨询、评价、数智安全及产品。E-mail:651906173@qq.com。

提取可以人工设计特征或使用机器学习技术进行自动化提取。为了提高网关的智能化和自动化程度,减少人工干预,根据评价协议识别算法优劣的标准进行综合权衡,基于机器学习的识别分类技术更适用于工控协议识别。

传统的机器学习技术采用云计算模式,为了解决云计算实时性不足、能耗大、数据隐私保密性较差等问题,面向网络边缘的数据计算模式——边缘计算应运而生。随着边缘计算的发展,人工智能也逐渐迁移到边缘,即边缘智能。边缘智能在发展中面临的主要阻碍是人工智能算法需要较强的算力支持,然而相比于云计算,边缘设备的计算能力较低,因此无法直接将人工智能算法迁移至边缘。在边缘智能场景下应用协同计算技术可以有效地解决上述问题。

因此,现提出一种基于边缘分布式深度学习的工控协议识别方法,将卷积神经网络模型应用于工控协议数据的识别和分类,并通过边缘计算实现分布式协同训练。具体来说,首先需要收集和预处理工控网络中的真实协议数据。然后,选择合适的卷积神经网络模型,通过隐式提取协议的本质特征,实现对多种工控协议的准确分类和识别,为边缘智能的发展提供技术支撑。

# 1　协议识别技术与协同训练技术

## 1.1　基于机器学习的协议识别技术

目前,基于机器学习主要包括有监督学习、无监督学习和半监督学习三类方法。其中,有监督学习在协议识别中的应用广泛,主要包括朴素贝叶斯方法[1](naive bayes, NB)、支持向量机[2-3](support vector machine, SVM)、决策树(C4.5)、神经网络(neural network, NN)等。其中,NB 方法计算简单,适用于大规模数据集,然而这种方法假设属性之间相互独立,实际应用中这种假设不总是成立。SVM 能够处理高维数据,分类效果好,尤其适用于小样本集,但其计算复杂度高,训练时间较长。决策树易于理解和解释,能够处理不均衡数据,但容易过拟合。神经网络具有较强的表征学习能力,能够自动提取数据特征,且能够规避以上方法的问题。

通过实验对比发现,神经网络(neural network, NN)在协议识别中表现出良好的性能,其中卷积神经网络(convolutional neural network, CNN)效果最佳,符合实际应用标准。2017 年提出一种基于 CNN 的恶意软件流量分类技术[4]。该技术利用 CNN 进行表征学习,具有较高扩展性,准确度符合应用标准。Luo 等[5]采用潜在狄利克雷分布 LDA 模型,通过推断每条消息的类型分布,使用类型和 n-gram 来表征消息,类型分布最终用于衡量消息之间的相似性,依据相似性进行协议识别。Kleber 等[6]通过比较特征向量来测量相似性,结合 Hirschberg 对齐算法与 DBSCAN 聚类算法,提出了一种新颖的推断机制,更好地识别协议类别。Meng 等[7]提出了一种新颖的框架,旨在解决针对各种流量分类任务的数据包表示学习问题。通过对比损失和样本选择器优化学习到的表示,使相似的数据包在潜在语义空间中更加接近,有效识别协议类型。何迎利等[8]为提升网络流量预测精度,提出了一种局部上下文信息增强的注意力机制,通过卷积计算优化 $Q$ 和 $K$ 的生成,增强时间序列的局部感知能力。该机制结合 LSTM 和 GRU 模型,显著提高了协议预测精度。朱本科等[9]为解决无线传感器网络分簇路由协议中簇头节点位置分布不均和数据传输路径不合理问题,提出基于改进社交网络搜索算法优化模糊 $C$ 均值聚类的动态分簇路由协议,提高了网络协议识别效率和网络负载均衡性。

## 1.2　基于机器学习的协同训练技术

分布式协同训练技术通过将神经网络训练任务分散到多个计算节点上,以提高训练速度和模型性能。这种技术尤其适用于边缘计算和云计算环境,能够有效解决计算资源不足和训练效率低下的问题。

Lu 等[10]设计了一种基于神经架构搜索的定制化网络架构,用于自适应地进行神经网络搜索,充分利用边缘服务器的计算资源。Wang 等[11]提出了一种名为 IndustEdge 的边缘-云协同智能(edge-cloud collaborative intelligence, ECCI)平台。该平台将时间敏感网络(time-sensitive networking, TSN)作为链路层的确定性传输方式,并提供可扩展的 ECCI 编排组件以减少系统级的协同训练延迟。Jian 等[12]提出了一种基于云边协同的两级混合协同训练模型,随后提出了一种带有干扰因子和可变步长的改进蝙蝠调度算法(variable step size bat algorithm, VSSBA)。然后,根据历史调度数据,提出了改进的长短期记忆网络(long short-term memory network, LSTM)模型,用于快速预测云边协同结果。Wang 等[13]设计了一种基于移动边缘设备的数据收集协议。通过该协议,计算范式从集中式云端转向分布式边缘,并利用了异构设备的差异化能力,该框架能够在资源紧张的 IoT 边缘集群上自适应地执行。Yang 等[14]提出了一种适用于边缘侧和云端的高效智能协同模型,为边缘节点的动态管理提供了理论基础,同时,还设计了一种端-边-云框架,优化

了数据处理效率和节点部署,同时最大化了 IoT 的智能水平并实现了节点的智能化管理。

赵婵婵等[15]为了减少资源受限的移动边缘计算场景下任务卸载和资源分配过程中的能量消耗,提出缓存辅助的动态卸载决策和计算、通信、缓存多维资源分配的联合优化策略,在资源约束条件下有效提升了系统性能。张晓龙等[16]针对传统云计算难以满足 5G 网络需求的问题,提出基于移动边缘计算框架的联合优化卸载策略,综合考虑通信时延与计算时延进行任务决策,有效降低了卸载时间,提高了数据处理能力。姚楠等[17]针对传统卸载模型在云端资源利用上的局限性,提出基于深度强化学习的边云协同计算任务卸载与资源配置优化算法,综合优化时延、能耗及能效模型,显著降低计算时延和能耗。

在工控协议识别领域,现有的研究方法主要集中在云计算和机器学习技术的应用上。然而,这些方法存在以下不足之处:实时性不足,传统云计算模式由于需要将数据上传至云端进行处理,导致数据传输延迟,无法满足工控系统对实时性的高要求;能耗高,云计算模式需要大量的计算资源和能源支持,这在实际应用中成本较高;数据隐私和安全问题,将数据上传至云端处理存在数据泄露的风险,无法有效保障工控系统的数据隐私和安全。适应性差,现有方法在面对工控行业大量非标准协议时,识别准确性和效率较低,无法满足实际需求。

为了解决以上问题,现提出一种边缘分布式深度学习的工控协议识别方法,采用边缘计算和分布式协同训练,通过在边缘计算集群上进行数据并行处理,有效减少数据传输延迟,保证系统的实时性,并通过边缘计算集群的协同训练,减少对中心服务器的依赖,降低了能耗和成本,同时由于数据在边缘设备上处理,提升数据隐私保护,不仅提高识别准确率和训练效率,还通过边缘计算实现实时性和数据隐私保护,为工控系统的安全保护提供有效技术手段,并为边缘智能的发展提供新的思路。

## 2 一种基于卷积神经网络技术的工控协议识别方法

### 2.1 模型设计

以 LeNet-5 为模板,对其进行改动,设计了适用于工控协议识别的优良模型。该卷积神经网络模型包含 7 层,分别为输入层、C1 层(卷积层)、S2 层(池化层)、C3 层、S4 层、FC5(全连接层)层和输出层。

在卷积过程中,图像逐渐缩小,直到卷积结束。由于边缘点的计算次数较少,会导致图像边缘信息的丢失,为解决这个问题,通常使用填充(padding)方法,在卷积前在图像外围填充 0,使卷积后的特征图像大小与原始图像一致。这种方式被称为“Same padding”,而不填充的方式则被称为“Valid padding”。在卷积中,常用的激活函数有 sigmoid、ReLU 和 tanh 等。LeNet-5 采用 tanh 作为激活函数,其公式为

$$\tanh(x) = \frac{e^{x} - e^{-x}}{e^{x} + e^{-x}} \tag{1}$$

式(1)中:$x$ 为输入值。

然而,由于 tanh 在接近饱和时导数趋近于 0,易出现梯度消失的情况,因此本文研究中选择 ReLU 函数作为激活函数更为合适,因为在大于 0 时,ReLU函数的导数始终为 1,其公式为

$$\mathrm{ReLU}(x) = \max(0,x) \tag{2}$$

在输出层中,由于工控协议识别本质上是一个多分类问题,因此选择常用于多分类的 Softmax 函数。Softmax 将 $x$ 分类为类别 $k$ 的概率为

$$p(\boldsymbol{y}^{i} = k \mid \boldsymbol{x}^{i};\boldsymbol{\theta}) = \frac{e^{\boldsymbol{\theta}_k^{\mathrm{T}}\boldsymbol{x}^{i}}}{\sum_{l=1}^{K} e^{\boldsymbol{\theta}_l^{\mathrm{T}}\boldsymbol{x}^{i}}} \tag{3}$$

式中:$\boldsymbol{x}^{i}$ 为第 $i$ 个样本的特征向量;$\boldsymbol{y}^{i}$ 为第 $i$ 个样本的真实类别;$\boldsymbol{\theta}$ 为模型参数;$\boldsymbol{\theta}_k$ 、$\boldsymbol{\theta}_l$ 为第 $k$、$l$ 个类别权重向量。

此外,为了防止模型过拟合问题,本文研究采取 dropout 方法确保模型中每一个节点的权重不会过大,因此设置了一个节点丢弃概率 $q$。即,每个神经节点都有 $q$ 的可能性被丢弃,然后通过遍历将其应用于神经网络中的每一层节点。其工作原理如图 1 所示。

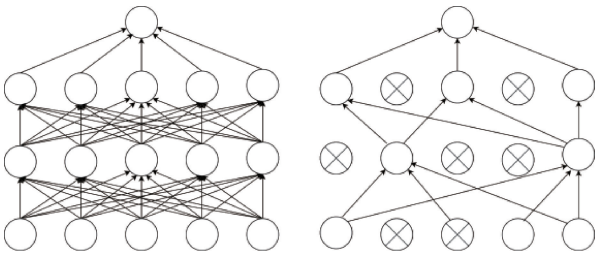

图 1 dropout 工作原理

Fig. 1 Working principle of dropout

### 2.2 模型结构

实验基于 LeNet-5 设计了 6 种不同的卷积神经网络结构,如表 1 所示,其中 C1 层与 C3 层数值含义表示为层数 ×(像素 × 像素),S2 层与 S4 层数值

含义表示为(像素 × 像素)。6 种结构分别对 C1 卷积层采用 8、16、32 个卷积核,对 C3 卷积层采用 16、32、64 个卷积核,对 FC5 全连接层采用 128、256 个神经元,进行了不同模型识别准确率的对比,以寻找最合适的卷积神经网络结构。以编号为 6 的结构为例,卷积神经网络模型总体结构如图 2 所示。

Input 层是输入层,模型输入数据为 28 × 28 的特征图片。C1 层为 1 号卷积层,设置卷积核大小为 5 × 5,数量为 32,采取 Same padding 模式卷积输入特征图,加上偏置项后使用 ReLU 函数激活,输出 32 张 28 × 28 的特征图片。S2 层为 1 号池化层,选取 Max pooling 方式,池化窗口大小为 2 × 2,输出 32 张 14 × 14 的特征图片。C3 层为 2 号卷积层,设置卷积核大小为 5 × 5,数量为 64,采取 Same padding 模式卷积输入特征图,加上偏置项后使用 ReLU 函数激活,输出 64 张 14 × 14 的特征图片。S4 层为 2 号池化层,选取 Max pooling 方式,池化窗口大小为 2 × 2,得到 64 张 7 × 7 的特征图片。FC5 层为全连接层,包含 256 个神经元,选取 ReLU 函数激活,并使用 dropout 策略。Output 层为输出层,选取 Softmax 函数作为分类器,输出 7 类工控协议。

**表 1　6 种卷积神经网络结构**

**Table 1　6 types of convolutional neural network structures**

| 编号 | C1 层 | S2 层 | C3 层 | S4 层 | FC5 层数量 |
|---|---|---|---|---|---|
| 1 | 8 × (5 × 5) | 2 × 2 | 16 × (5 × 5) | 2 × 2 | 128 |
| 2 | 8 × (5 × 5) | 2 × 2 | 16 × (5 × 5) | 2 × 2 | 256 |
| 3 | 16 × (5 × 5) | 2 × 2 | 32 × (5 × 5) | 2 × 2 | 128 |
| 4 | 16 × (5 × 5) | 2 × 2 | 32 × (5 × 5) | 2 × 2 | 256 |
| 5 | 32 × (5 × 5) | 2 × 2 | 64 × (5 × 5) | 2 × 2 | 128 |
| 6 | 32 × (5 × 5) | 2 × 2 | 64 × (5 × 5) | 2 × 2 | 256 |

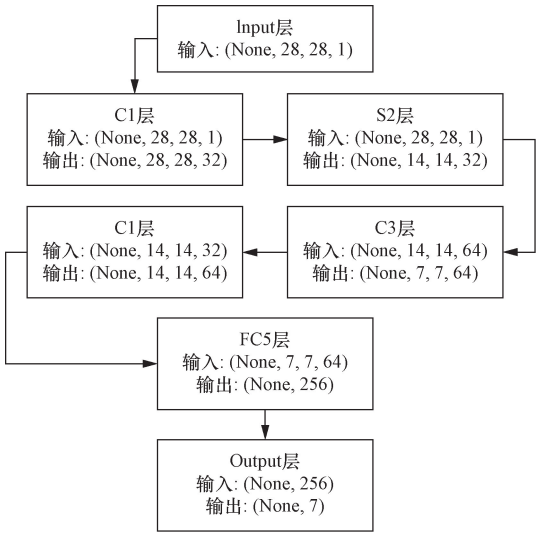


图 2　模型总体结构

Fig. 2　Overall structure of the model

## 3　实验结果与分析

工控协议的识别流程大体可分为 6 个阶段:数据采集、数据预处理、特征提取、分类模型建立、模型验证和效果评估,如图 3 所示。

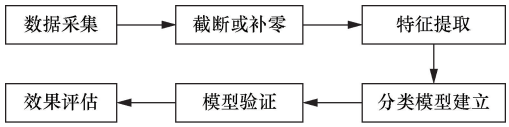


图 3　工控协议识别流程

Fig. 3　Industrial control protocol identification process

### 3.1　数据预处理

本次实验对网络中开放的工控网络流量数据进行采集,数据格式为 pcap 网络流量包。在采集到的数据中存在噪音数据,如普通 TCP、SMTP 类型的非工控协议数据,使用 Wireshark 软件对数据集进行筛选、组合、分割,共整理出 7 种常见工控协议类型,有效数据约 $7 \times 10^4$ 条,数据充足且全面。由于采集到的 pcap 网络流量包不能直接作为卷积神经网络输入数据使用,需要提取原始数据中的有效信息,并转化成适用于卷积神经网络的输入数据格式,因此需要进行数据预处理操作。

数据流分类按照 7 种工控协议类型,通过使用 Wireshark 软件的筛选、组合、分割、去重等功能,将不同协议类型的数据分别保存于新的 pcap 文件中,以便后续对单一协议数据帧的处理。数据帧处理以二进制流读取每个 pcap 文件时,开始的 24 字节为 pcap 文件头(Pcap Header),之后是多个数据帧(Packet)。在每个数据帧中,开始 16 字节为数据帧头(Packet Header),其中字节 0 ~ 4 表示数据帧捕获时间戳高位;字节 5 ~ 8 表示数据帧捕获时间戳低位;字节 9 ~ 12 表示当前数据帧长度,以此可以得到下一数据帧位置;13 ~ 16 字节表示网络实际数据帧长度。对于每一数据帧头,其后为数据帧数据(Packet Data)。对于每条数据帧数据,开始 14 字节是表示以太网头部,其中字节 0 ~ 5 表示目的地址,字节 6 ~ 11 表示源地址。由于需要提取出不同工控协议的特征信息,因此选取从字节 12 开始的剩余数据。数据帧数据处理需要将数据帧数据转化为卷积神经网络接受的输入数据格式。首先,将由 0x00-0xff 十六进制字节表示的数据转化为 0 ~ 255 的十进制表示,以此对应图片中的 0 ~ 255 像素值。工控协议数据取值范围较大,取值分布较为分散,因此,将协议数据进行归一化处理(Normalization),规范数据范围为[0,1],同量级化数据,便于模型训练。与协议类型相关的重要数据位置,选择数据前部长度 $L = 784$ 作为输入。对于超过 784 字节的数据进行截断,不足 784

字节的数据在末尾添加 0×00,进行补零处理(zero padding)。最后,将长度为 784 字节的一维向量转为卷积神经网络输入数据类型,即 28 × 28 的二维矩阵。以 EtherCAT 与为例,经过处理后的不同协议数据表现出不同的图片特征。

之后,将包含 7 种工控协议的数据集分别按照类型打上 0~6 的标签,由于协议数据属于离散型数据,one-hot 标签更适用,因此将标签转为 one-hot 标签。例如,当协议数据共有 7 种时,则该协议的标签设置为一个 7 维向量,若某一数据属于第 4 种协议,那么对应标签为$[0,0,0,1,0,0]^{T}$,其中第 4 位取值为 1,表示对应的第 4 种协议,其余位为 0。

此外,由于不同工控协议的开放性不一致,因此收集到的工控协议数据存在不均衡的问题,即数据集长尾分布问题,如收集到的 ModBus 数据 40 000 余条,而 EtherCAT、DNP 3.0 数据仅 1 000 余条。本文研究中采取少数类数据采取 Border-line SMOTE 方法[18]增加数据量。该方法是一种常用于解决数据集不均衡的随机生成少数类的过采样方法。SMOTE 方法[19-20]通过综合现有数据生成新的少数类数据。该算法通过对目标类及其邻域特征空间的采样,将目标类的特征与其邻域特征相结合,生成新的实例。Border-line SMOTE 方法在使用 SMOTE 算法合成正实例时将边界因素纳入考虑,是 SMOTE 算法基础上的优化算法。该方法利用每个少数实例的多数邻居数,将少数实例分成 3 组:①安全组,指该实例所有的最近邻实例与其类别一致;②危险组,指≥50% 的最近邻实例与该实例类别不一致;③噪声组:指所有最近邻实例全部来自不同于该少数实例的其他类。

Border-line SMOTE 算法随机选择处于危险中的实例,然后用 SMOTE 算法产生新的实例。经过数据均衡处理,最终数据集中每条工控协议数据量及编号如表 2 所示。

最后,随机打乱生成的数据集,选取 80% 的数据作为训练集,20% 作为测试集。最终训练集与测试集的比例为 4:1。数据预处理总体流程如图 4 所示。

**表 2 工控协议数据集数量及编号**

**Table 2 Number and identification of industrial control protocol datasets**

| 协议类型 | 数量 | 编号 |
|---|---|---|
| BACnet | 10 000 | 0 |
| CIP PCCC | 10 000 | 1 |
| S7comm | 10 000 | 2 |
| ModBus | 10 000 | 3 |
| DNP 3.0 | 10 000 | 4 |
| PowerLink | 10 000 | 5 |
| EtherCAT | 10 000 | 6 |

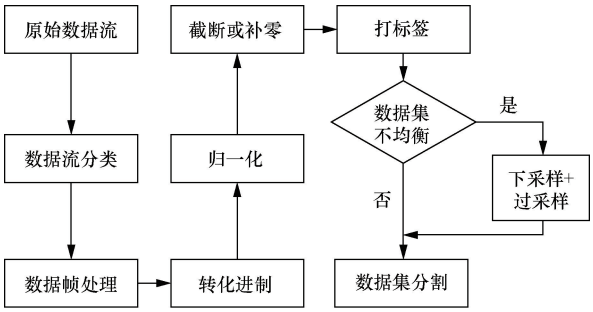


图 4 数据预处理流程

Fig. 4 Data preprocessing process

### 3.2 集群结构

本文研究使用 4 个树莓派 4B 单板机作为模拟边缘设备,树莓派使用网线直连交换机方式进行通信,从而搭建边缘分布式计算集群。

本文研究采取卷积神经网络数据并行结构,分别采取 1 Worker(单机)、1PS + 2 Worker(结构 1)、2PS + 2 Worker(结构 2)、1PS + 3 Worker(结构 3)4 种结构进行实验,参数更新采取异步更新方式,记录每次实验的总体识别准确率及训练时间。后 3 种并行分布式结构如图 5~图 7 所示。

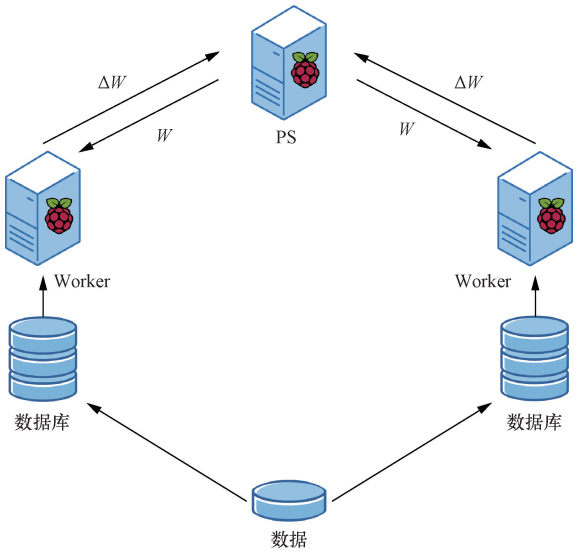


图 5 1PS + 2Worker

Fig. 5 1PS + 2Worker

### 3.3 实验结果

本文研究将工控协议识别模型得到的结果同真实结果作对比,采用模型识别总体准确率与模型训练时间作为评价指标。采取独立实验多次重复取平均值的方式,运行环境参数如表 3 所示。

首先针对 6 种 CNN 模型做了识别准确率的对比实验,实验结果如表 4 和图 8 所示。

由图 8 可见,在一定范围内随着卷积层中卷积核个数以及全连接层中神经元个数的增加,模型的

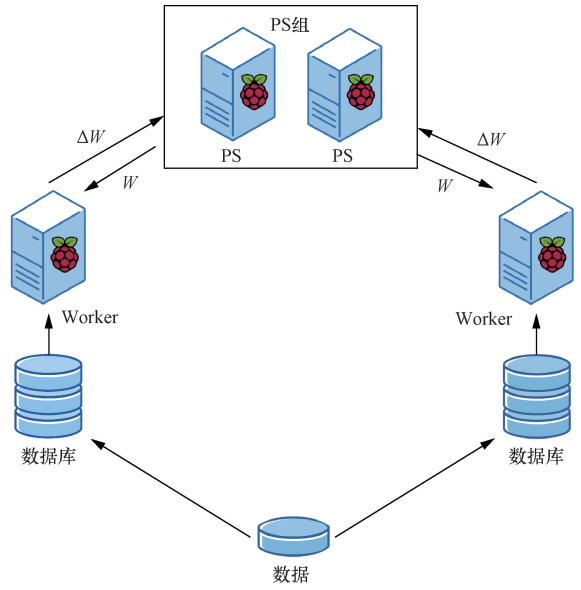


图 6　2PS + 2Worker

Fig. 6　2PS + 2Worker

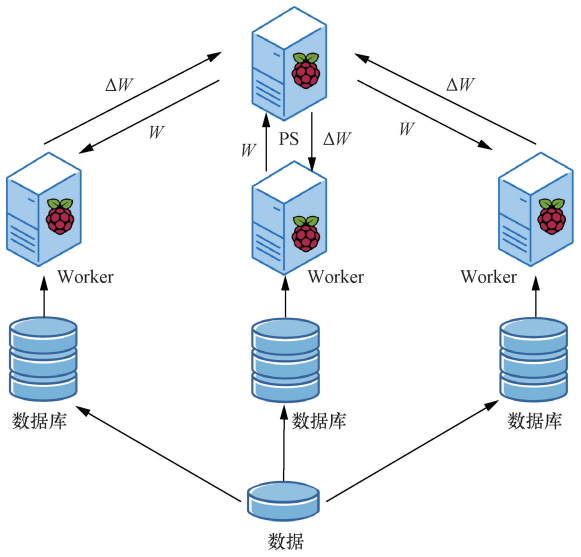


图 7　1PS + 3Worker

Fig. 7　1PS + 3Worker

**表 3　实验运行环境参数**

**Table 3　Experimental operating environment parameters**

| 类别 | 配置 |
|---|---|
| 硬件环境 | 树莓派 4B |
| 操作系统 | 基于 Debian 的 Raspberry Pi OS |
| 处理器 | ARM Cortex-A72 1.5 GHz |
| Tensorflow | 2.3.0 版本 |

**表 4　6 种不同 CNN 模型的实验结果**

**Table 4　Experimental results of 6 different CNN models**

| 编号 | 总体准确率/% | 编号 | 总体准确率/% |
|---|---|---|---|
| 1 | 97.50 | 4 | 99.58 |
| 2 | 98.67 | 5 | 99.67 |
| 3 | 99.13 | 6 | 99.92 |

总体识别准确率随之增加,编号为 6 的卷积神经网络模型总体识别准确率最高,达到 99.92%,该模型的训练过程中准确率变化、loss 值变化示例如图 9 和图 10 所示。

6 号模型的每一工控协议类别的单类识别结果(精准率、召回率)如表 5 所示。

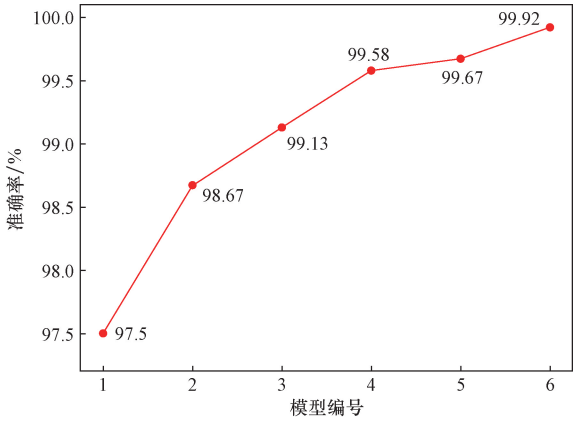


图 8　6 种 CNN 模型准确率对比图

Fig. 8　Comparison chart of accuracy of 6 CNN models

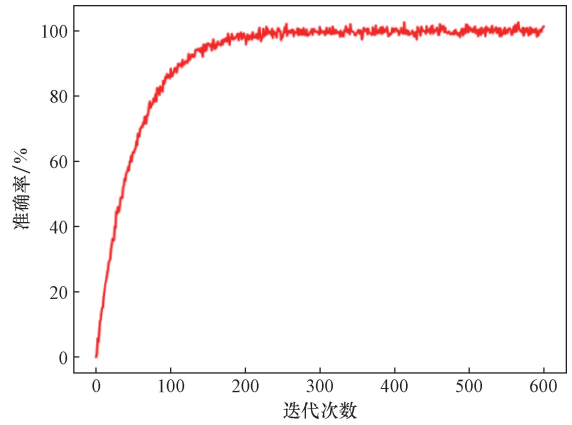


图 9　训练准确率变化图

Fig. 9　Training accuracy change chart

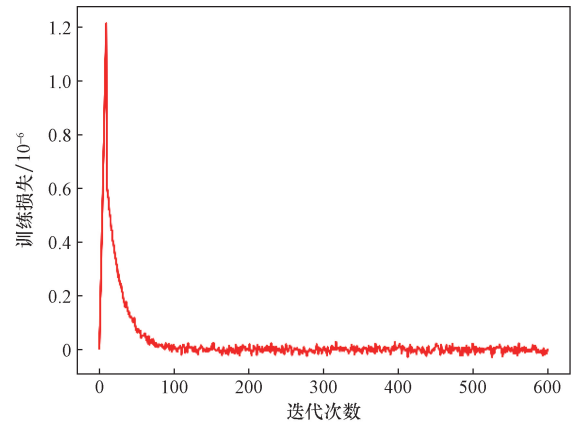


图 10　loss 值变化图

Fig. 10　The change chart of loss value

在实验中基于 6 号卷积神经网络结构对使用 dropout 和不使用 dropout 两种结构进行对比,实验结果如表 6 所示。

由表 6 可知,使用 dropout 的模型总体识别准确率要高于不使用 dropout 的模型识别准确率,dropout 可有效避免模型的过拟合问题,实验中 dropout 策略的节点保留概率设置为 0.75。

分别对 4 种不同的集群结构进行了对比实验,4 种结构平均识别总体准确率与训练时间如图 11 所示。实验结果显示,分布式环境中,在保证总体识别准确率的前提下,1PS + 2Worker 分布式结构可以提升训练速率 1.87 倍,1PS + 3Worker 分布式结构可以提升训练速率 2.81 倍,2PS + 2Worker 结构与 1PS + 2Worker 结构对训练速率的提升效率几乎相同。

**表 5 单类识别结果**

**Table 5 Single class recognition result**

| 编号 | 协议类型 | 测试数量 | 准确率/% | 召回率/% |
|---|---|---|---|---|
| 0 | BACnet | 1 004 | 99.70 | 99.90 |
| 1 | CIP PCCC | 1 028 | 99.32 | 100.00 |
| 2 | S7comm | 981 | 99.90 | 99.90 |
| 3 | ModBus | 1 003 | 100.00 | 99.90 |
| 4 | DNP 3.0 | 986 | 99.90 | 99.29 |
| 5 | PowerLink | 987 | 100.00 | 100.00 |
| 6 | EtherCAT | 1 011 | 99.90 | 99.70 |

**表 6 dropout 对模型识别的影响结果**

**Table 6 The impact of dropout on model recognition results**

| 是否使用 dropout | 总体准确率/% |
|---|---|
| 使用 | 99.92 |
| 不使用 | 99.17 |

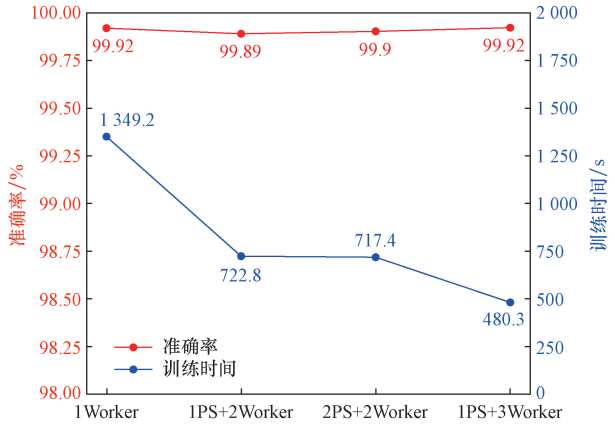


图 11 训练准确率变化图

Fig. 11 Training accuracy change chart

## 4 结论

提出了一种基于边缘分布式深度学习的工控协议识别方法,利用优化的卷积神经网络和边缘计算技术,为工业控制协议识别问题提供了创新解决方案。得出如下结论。

(1)本文提出的分布式深度学习的架构能够有效应对工业控制网络中的多样化非标准协议识别问题,显著提升准确率和实时响应能力。

(2)本文提出的优化的卷积神经网络结构进一步提高了协议识别的精度,最高可达 99.92%。

(3)本文提出数据并行分布式训练方法显著提升了模型训练效率,满足工业环境对实时性和效率的高要求。

(4)本文方法在提升协议识别效率、降低能耗及数据隐私保护方面具有显著优势,为工业控制系统的安全保护和智能化发展提供了技术支撑。

## 参 考 文 献

[1] Kumar R, Swarnkar M, Singal G, et al. IoT network traffic classification using machine learning algorithms: an experimental analysis [J]. IEEE Internet of Things Journal, 2021, 9(2): 989-1008.

[2] Dong S. Multi class SVM algorithm with active learning for network traffic classification[J]. Expert Systems with Applications, 2021, 176. DOI: 10.1016/j.eswa.2021.114885.

[3] AlZoman R M, Alenazi M J F. A comparative study of traffic classification techniques for smart city networks[J]. Sensors, 2021, 21(14). DOI: 10.3390/s21144677.

[4] Wang W, Zhu M, Zeng X, et al. Malware traffic classification using convolutional neural network for representation learning[C]// International Conference on Information Networking (ICOIN). Danang: IEEE, 2017: 712-717.

[5] Luo X, Chen D, Wang Y, et al. A type-aware approach to message clustering for protocol reverse engineering[J]. Sensors, 2019, 19(3). DOI:10.3390/s19030716.

[6] Kleber S, van der Heijden R W, Kargl F. Message type identification of binary network protocols using continuous segment similarity [C]//IEEE INFOCOM 2020-IEEE Conference on Computer Communications. New York: IEEE, 2020: 2243-2252.

[7] Meng X, Wang Y, Ma R, et al. Packet representation learning for traffic classification[C]//Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Washington: Association for Computing Machinery, 2022: 3546-3554.

[8] 何迎利, 胡光宇, 张浩, 等. 基于局部信息增强注意力机制的网络流量预测[J]. 科学技术与工程, 2023, 23(30): 13014-13022.
He Yingli, Hu Guangyu, Zhang Hao, et al. Network traffic prediction based on local information enhanced attention mechanism[J]. Science Technology and Engineering, 2023, 23(30): 13014-13022.

[9] 朱本科, 高丙朋, 蔡鑫. 基于多因素均衡动态分簇的 WSN 路由协议算法研究[J]. 科学技术与工程, 2024, 24(16): 6799-6808.
Zhu Benke, Gao Bingpeng, Cai Xin. Research on WSN routing protocol algorithm based on multi-factor balanced dynamic clustering

[J]. Science Technology and Engineering, 2024, 24(16): 6799-6808.

[10] Lu H, Du M, He X, et al. An adaptive neural architecture search design for collaborative edge-cloud computing[J]. IEEE Network, 2021, 35(5): 83-89.

[11] Wang Y, Yang S, Ren X, et al. IndustEdge: a time-sensitive networking enabled edge-cloud collaborative intelligent platform for smart industry[J]. IEEE Transactions on Industrial Informatics, 2021, 18(4): 2386-2398.

[12] Jian C, Ping J, Zhang M. A cloud edge-based two-level hybrid scheduling learning model in cloud manufacturing [J]. International Journal of Production Research, 2021, 59(16): 4836-4850.

[13] Wang T, Zhao D, Cai S, et al. Bidirectional prediction-based underwater data collection protocol for end-edge-cloud orchestrated system[J]. IEEE Transactions on Industrial Informatics, 2019, 16(7): 4791-4799.

[14] Yang Z, Liang B, Ji W. An intelligent end-edge-cloud architecture for visual IoT-assisted healthcare systems[J]. IEEE Internet of Things Journal, 2021, 8(23): 16779-16786.

[15] 赵婵婵, 郭晓敏, 海晓伟, 等. 缓存辅助移动边缘计算的任务卸载与资源分配联合优化策略[J]. 科学技术与工程, 2023, 23(9): 3812-3819.
Zhao Chanchan, Guo Xiaomin, Hai Xiaowei, et al. Joint optimization strategy of task offloading and resource allocation for cache-assisted mobile edge computing[J]. Science Technology and Engineering, 2023, 23(9): 3812-3819.

[16] 张晓龙, 吴巍, 周彬. 基于移动边缘计算的任务卸载策略研究[J]. 科学技术与工程, 2022, 22(11): 4434-4439.
Zhang Xiaolong, Wu Wei, Zhou Bin. research on the motion recognition method of lower limb rehabilitation training robot for the elderly[J]. Science Technology and Engineering, 2022, 22(11): 4434-4439.

[17] 姚楠, 刘子全, 秦剑华, 等. 基于电力物联网的边缘计算任务卸载优化[J]. 科学技术与工程, 2022, 22(16): 6577-6584.
Yao Nan, Liu Ziquan, Qin Jianhua, et al. Offloading optimization of the edge computing task based on the power internet of things [J]. Science Technology and Engineering, 2022, 22(16): 6577-6584.

[18] Sun Y, Que H, Cai Q, et al. Borderline smote algorithm and feature selection-based network anomalies detection strategy [J]. Energies, 2022, 15(13): 4751.

[19] Soltanzadeh P, Hashemzadeh M. RCSMOTE: range-controlled synthetic minority over-sampling technique for handling the class imbalance problem [J]. Information Sciences, 2021, 542: 92-111.

[20] Liu J. Importance-SMOTE: a synthetic minority oversampling method for noisy imbalanced data[J]. Soft Computing, 2022, 26(3): 1141-1163.