

成绩_____

苏州大学

课 程 _____ 文献阅读和科技写作

学院(部) _____ 计算机科学与技术学院

类 型 _____ 专题文献查找

学 号 _____ 1927405160

姓 名 _____ 张昊

日 期 _____ 2022 年 3 月 3 日

专题文献查找

1927405160 张昊

1(苏州大学 计算机科学与技术学院, 江苏 苏州 215006)

1. 专题题目

边缘计算中的联邦学习

2. 专题背景、查找以及筛选过程

2.1. 研究意义

现代机器学习方法（如深度学习）基本都需要大量的数据来训练准确和稳健的模型。然而，在现实生活中，无论是中小型企业、科研院所都存在数据量少，数据质量差的问题，不足以支撑深度学习等人工智能技术的实现；同时在国内监管环境下对数据的保护意识日益提升，出台了许多相关政策。在这一背景下，出现了联邦学习（Federated Learning），其设计目标是在数据不发生流动、保护终端数据和个人数据隐私、保证合法合规的前提下，在多参与方或多计算结点之间开展高效率的机器学习。

随着 5G 时代的到来，密集的无线终端可以更多地参与到模型训练中，训练数据通常以分布式的形式产生和存储在不同用户设备局部中。因此，在网络边缘利用联邦学习，可以充分利用终端节点的计算资源，并能够在保护用户个人信息的前提下，进行更广泛和高效的机器学习。然而，这也给联邦学习带来了更多新的挑战：存在于终端设备中的数据往往是非独立同分布的，各终端的计算能力也不尽相同，不稳定的通信条件也会进一步影响模型训练，在网络上的联邦学习可能受到攻击，等等。在边缘计算场景中，如何克服上述问题，提升联邦学习的性能与安全值得进一步分析与研究。

2.2. 文献检索

结合上一小节有关选题背景与研究意义的讨论，总结出“联邦学习（federated learning）”、“边缘计算（edge computing）”、“边缘网络（edge networks）”、“通信高效（communication

efficient) ”、“物联网 (Internet of Things, IoT) ”、“资源受限 (resource constrained) ”六个关键词。以“联邦学习 (federated learning) ”作为主要关键词, 排列组合其他五个关键词, 在 DBLP 数据库 (<https://dblp.uni-trier.de/>) 以及谷歌学术 (<https://scholar.google.com/>) 中进行有关文献的检索。

2.3. 文献筛选

通过阅读检索到的文献的题目以及摘要等信息, 对其进行筛选, 共选择了 12 篇文献。下面针对每一篇文献说明筛选理由。

文献[1]、[2]、[3]均选取了联邦学习的综述。其中文献[1]题为“资源受限物联网设备的联邦学习研究”, 文献[3]题为“物联网联邦学习——最新进展、分类和开放挑战”, 均是物联网领域的联邦学习综述, 题目中包含了“联邦学习 (federated learning) ”、“物联网 (Internet of Things, IoT) ”、“资源受限 (resource constrained) ”等关键词。文献[2]题为“联邦机器学习——通信和网络系统中的调查, 多层次分类, 理想标准和未来方向”, 包含关键词“联邦学习 (federated learning) ”、“通信与网络 (communication and networking) ”, 同时通过阅读摘要了解到, 这是一篇较为详尽的联邦学习综述, 可以对联邦学习有一个较为全面的认识。

其余文献的选取侧重于边缘计算中联邦学习的一些具体问题, 选取的大部分文献的研究目标为资源受限环境下对联邦学习方法的改进与优化。这些文献均包含“通信高效 (communication efficient) ”等关键词, 且在选择为阅读文献时都有根据摘要中找到其创新点或值得阅读的参考价值。文献[4]题为“资源受限边缘计算系统中的自适应联邦学习”, 其问题背景为从分布在多个边缘节点的数据中学习模型参数的问题, 与选题契合度较高; 且提出了一种可以在给定资源预算下的自适应控制算法, 具有参考价值。文献[5]题为“资源受限的边缘计算中通信高效的异步联邦学习”, 指出了原有的联邦学习框架不能很好地应用于资源受限的边缘节点, 提出了通信高效的异步联邦学习机制, 并证明了其方法的收敛性, 因此选为翻译文献。文献[6]题为“基于不平衡数据的物联网异构系统中通信高效的层次联邦学习”, 针对物联网异构系统提出了一种基于分层联邦学习体系结构的分配优化方案, 具有一定的参考价值。文献[7]题为“基于去中心化数据的深度网络的高效通信学习”, 这篇文献中谷歌提出了在安卓手机端实现带有隐私保护的横向联邦学习, 较早地 (2017 年) 提出了边缘计算中的联邦学习; 且其提出的联邦平均 (FedAvg) 方法被后续文献广泛作为基线方法进行比较, 具有较高的参考价值。文献[8]题为“工业物联网中数字孪生边缘网络的通信高效的联邦学习”, 将数字孪生整合到边缘网络中, 利用联邦学习来构建数字孪生模型, 创新点新颖。文献[9]题为“物联网中

无线边缘智能的通信高效联邦学习”，这篇文献是对联邦平均方法的改进，且应用场景与选题契合。文献[10]题为“一种降低通信成本的新型联邦学习方法定义”，其验证是基于一个医疗案例研究，在性能和通信成本方面取得了很好的结果。文献[11]题为“基于联合模型剪枝和设备选择的通信高效的联邦边缘学习”，这篇文献在无线联邦学习中引入了模型剪枝来减小神经网络的规模，具有一定的参考价值。

此外，还选择了少部分有关联邦学习安全性的文献。文献[12]题为“联邦学习框架下的隐私和安全保护”，其中分析了隐私和安全问题，指出一些针对联邦学习架构的攻击仍然可以提取隐私信息，可以作为选题参考文献的补充。

3. 专题相关的文献列表（至少 10 篇，翻译加粗）

- [1] Imteaj A, Thakker U, Wang S, *et al.* A survey on federated learning for resource-constrained IoT devices. *IEEE Internet of Things Journal*, 2021, 9(1): 1-24.
- [2] Wahab O A, Mourad A, Otrók H, *et al.* Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. *IEEE Communications Surveys & Tutorials*, 2021, 23(2): 1342-1397.
- [3] Khan L U, Saad W, Han Z, *et al.* Federated learning for internet of things: Recent advances, taxonomy, and open challenges. *IEEE Communications Surveys & Tutorials*, 2021, 23(3): 1759-1799.
- [4] Wang S, Tuor T, Salonidis T, *et al.* Adaptive federated learning in resource constrained edge computing systems. *IEEE Journal on Selected Areas in Communications*, 2019, 37(6): 1205-1221.
- [5] **Liu J, Xu H, Xu Y, *et al.* Communication-efficient asynchronous federated learning in resource-constrained edge computing. *Computer Networks*, 2021, 199: 108429.**
- [6] Abdellatif A A, Mhaisen N, Mohamed A, *et al.* Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced data. *Future Generation Computer Systems*, 2022, 128: 406-419.
- [7] McMahan B, Moore E, Ramage D, *et al.* Communication-efficient learning of deep networks from decentralized data//*Artificial Intelligence and Statistics*. Fort Lauderdale, USA, 2017: 1273-1282.

- [8] Lu Y, Huang X, Zhang K, *et al.* Communication-efficient federated learning for digital twin edge networks in industrial IoT. *IEEE Transactions on Industrial Informatics*, 2020, 17(8): 5709-5718.
- [9] Mills J, Hu J, Min G. Communication-efficient federated learning for wireless edge intelligence in IoT. *IEEE Internet of Things Journal*, 2019, 7(7): 5986-5994.
- [10] Paragliola G, Coronato A. Definition of a novel federated learning approach to reduce communication costs. *Expert Systems with Applications*, 2022, 189: 116109.
- [11] Liu S, Yu G, Yin R, *et al.* Joint model pruning and device selection for communication-efficient federated edge learning. *IEEE Transactions on Communications*, 2021, 70(1): 231-244.
- [12] Ma C, Li J, Ding M, *et al.* On safeguarding privacy and security in the framework of federated learning. *IEEE Network*, 2020, 34(4): 242-248.