计算机科学
COMPUTER SCIENCE

群体智能中的协作与对抗

朱迪迪, 吴超

引用本文

朱迪迪, 吴超. 群体智能中的协作与对抗[J]. 计算机科学, 2022, 49(11A): 210900249-7.

ZHU Di-di, WU Chao. Cooperation and Confrontation in Crowd Intelligence[J]. Computer Science, 2022, 49(11A): 210900249-7.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210900249

群体智能中的协作与对抗

朱迪迪[1]　吴　超[2]
1 浙江大学计算机科学与技术学院　杭州 310013
2 浙江大学公共管理学院　杭州 310058
(didi_zhu@zju.edu.cn)

摘　要　群体智能有着丰富的内涵和外延,其算法既包括早期基于生物群体特征规律的算法(粒子群优化和蚁群算法等),也包括后期基于网络互联的大规模群体算法(多智能体系统、群智感知和联邦学习等)。这些群体智能算法均蕴含着协作或对抗的核心思想。协作能够把个体的有限智慧耦合汇聚成群体的强大智能,但是协作本身具有一定的局限性,可能会导致个体间过分依赖和系统的不公平性等问题。对抗可以突破这种局限性,其基本思想是个体通过博弈等手段谋取自身最大利益。因此,协作和对抗缺一不可,以对抗促协作,协作中存对抗。通过聚焦群体智能算法的协作和对抗方法,对经典群体智能算法的思想进行阐述,并对新兴的群体智能算法的下一步发展方向进行展望,总结了构建协作与对抗并存的群体智能生态,是群体智能的必然发展趋势。

关键词:群体智能;联邦学习;多智能体系统;对抗;博弈
中图法分类号　TP191

Cooperation and Confrontation in Crowd Intelligence

ZHU Di-di[1] and WU Chao[2]
1 College of Computer Science and Technology, Zhejiang University, Hangzhou 310013, China
2 School of Public Affairs, Zhejiang University, Hangzhou 310058, China

Abstract　Crowd intelligence has rich connotations and denotations. Its algorithms include both the early algorithms based on the characteristics of biological groups (particle swarm optimization, ant colony algorithm, etc.) and the later large-scale crowd algorithms based on network interconnection (multi-agent system, crowd intelligence perception, federated learning, etc.). The core idea of these crowd intelligence algorithms is cooperation or confrontation. Collaboration can combine the limited intelligence of individuals into the powerful intelligence of the group. However, collaboration itself has certain limitations, which may lead to the over-dependence between individuals and the unfairness of the system. Confrontation can overcome this limitation, and its basic idea is that individuals seek their maximum interests through the game. Therefore, cooperation and confrontation are indispensable. It is the inevitable development trend of a crowd intelligence to promote cooperation with confrontation, and to build a crowd intelligence ecology in which cooperation and confrontation coexist. This paper mainly focuses on the cooperation and confrontation methods of crowd intelligence algorithms, expounds on the classical crowd intelligence algorithms, and prospects the next development direction of emerging crowd intelligence algorithms.

Keywords　Crowd intelligence, Federated learning, Multi-agent system, Confrontation, Game

1　引言

近年来,人类对人工智能技术的研究主要聚焦于集中式个体智能,存在解决目标单一、约束环境静态等问题,尚不能达到大规模群体进行感知、预测和决策等目标。因此,群体智能[1]作为一种汇聚海量智能体来完成真实复杂任务的新范式,亟需被深入研究。

群体智能是由多个具有独立的问题解决能力和社会交互能力的个体构成的超越单个智能体的分布式系统。2017 年,群体智能在《新一代人工智能发展规划》中被列为重点发展的五大智能形态之一,在推动我国新一代人工智能技术发展中占据重要地位。因此,对群体智能的探究具有极高的战略意义和科研价值。

西北大学赵健等人指出,群体智能根据不同时代发展方向可以划分为两类——基于生物群体行为的群体智能和基于移动互联网的群体智能[2],并且首次将联邦学习[3]等新兴技术纳入后者。具体来说,早期群体智能算法主要是来源于对自然生态系统所具有智能的观察与表达,如蚁群优化算法[4]及粒子群优化算法[5]等。后期群体智能算法则是当前机器学习、大数据、物联网、隐私安全和博弈论等多研究领域交叉融合

基金项目:国家自然科学基金(U19B2042);浙江省自然科学基金一般项目(LY19F020051)
This work was supported by the National Natural Science Foundation of China(U19B2042) and Zhejiang Provincial Natural Science Foundation of China(LY19F020051).
通信作者:吴超(chao.wu@zju.edu.cn)

产生的一项新的技术，也是最具影响力的人工智能前沿研究领域之一。它的具体算法包括多智能体系统[6]、群智感知[7]、联邦学习[3]等技术。随着群体智能对安全和数据隐私提出了更高的需求，联邦学习作为一种新兴的隐私保护的群体智能算法，更是在近年来引起了社会界和工业界的广泛关注。

根据对群体智能算法的分析，本文总结出协作和对抗是群体智能算法的核心思想。群体智能中的协作能够确保全局模型性能接近参与方模型的平均性能。然而，在实际场景中，个体之间具有一定的差异性，其目标可能是彼此冲突的。如果仅从协作角度构建群体智能，就会产生不公平性等问题。这种智能体之间的差异性必然会打破完全协作状态。群体智能中的对抗可以通过智能体个性化来克服这种问题，从而实现系统的公平性。

本文认为，从协作走向对抗是群体智能发展的必经之路，我们应当构建协作与对抗机制并存的群体智能生态。本文首先对群体智能的总体发展历程进行介绍并明确群体智能的发展趋势，其次对体现协作和对抗思想的群体智能算法分别进行介绍，最后分析了新兴群体智能算法的主要研究方向。

2 群体智能

近年来，人工智能技术得到快速发展，在理论和应用领域都取得了重大突破。但作为一种仍在发展中的技术，人工智能还存在很多局限。目前，人工智能技术还停留在初级的集中式个体智能阶段，无法解决分散数据、复杂交互以及动态环境的变化等问题。在这种复杂环境下，大量智能体被连接起来，建模方式从集中式走向分布式，智能范式从个体智能走向群体智能，以“万物互联”为基础，走向“万物智能”。

2.1 群体智能概念

群体智能[1]最早在1989年由杰拉尔多等人针对细胞机器人的自组织现象所提出。大部分学者将其定义为：群体智能是具有分布式控制和去中心化特点的自组织智能。它是大规模多个体的协作与对抗中涌现出来的高级智能形态，在没有集中控制的前提下表现出了明显的优势。

群体智能具有下列4个特点。1)组织架构的分布式。群体不存在中心节点，个体不受集中控制，系统具有更强的安全性和隐私性。2)行为主体的简单性。群体中个体仅执行一项或几项简单的动作。3)环境适应的灵活性。个体在遇到环境变化时会通过网络互联和自适应调整适应环境。4)系统整体的智能性。个体通过环境反馈来改变自身动作，模型在分布式基础下不断迭代更新，能更好地适应外部环境的变化，具有智能性[8-9]。其中特点2)仅针对早期群体智能，在近期的群体智能技术中，个体的模型结构也越来越复杂。

2.2 早期群体智能

在群体智能发展之初，学者专注于研究生物群体行为特征规律，并针对这些行为特征提出一系列具备群体智能特征的算法。此类群体智能算法来源于自然领域中发现的“群体智能”。典型的早期群体智能算法包括蚁群优化算法、粒子群优化算法等。

2.2.1 蚁群优化算法

蚁群优化算法[4]由意大利学者多里戈于1991年提出，旨在解决旅行商问题。它是一种找优化路径的概率型算法。在研究蚂蚁觅食的过程中，多里戈发现单个蚂蚁的行为比较简单，但是蚁群整体却可以体现一些智能的行为。例如，蚁群可以在不同的环境下寻找到达食物源的最短路径。这是因为蚁群内的蚂蚁可以通过某种信息机制实现信息的传递。蚂蚁会在其经过的路径上释放信息素，蚁群内的蚂蚁会沿着信息素浓度较高路径行走，同时在路上留下信息素，从而形成一种类似正反馈的机制。

2.2.2 粒子群优化算法

粒子群算法[5]最初由美国普渡大学肯德迪和埃伯哈特于1995年提出，它的基本概念源于对鸟群觅食行为的研究。假设一群鸟在一定区域内随机搜寻食物，区域里有不同大小的食物，鸟群的任务是找到最大的食物源。鸟群在搜寻过程中通过相互传递位置信息，让其他鸟知道彼此位置，最终整个鸟群均能聚集在食物源周围，即达到最优解。基于这种自然界生物群体的观察，学者开发了诸多类似智能算法，如布谷鸟搜索算法[10]、鱼群算法[11]、狼群算法[12]等等。

2.3 近期群体智能

在人工智能技术蓬勃发展的新时代，海量的人类智能与机器智能相互赋能增效，形成人机物融合的“群智空间”。这为群体智能注入了新的活力，大大拓展了群体智能的研究领域与研究方法。北京大学Zhang等[13]指出群体智能的基本原理可以应用至网络互联的大规模人类群体，形成个体智能的放大效应，从而进一步释放人类社会的潜能，促进社会经济的发展。近期群体智能主要是基于移动互联网的群体智能，具体算法包括多智能体系统、群智感知、联邦学习等技术[2]。

2.3.1 多智能体系统

多智能体系统是一种博弈型的群体智能体系，其研究目的是解决大规模的、复杂的现实问题。多智能体系统自20世纪70年代被提出以来，就在智能机器人、交通控制、分布式决策、虚拟现实等各个领域迅速得到了应用。多智能体系统的代表方法是多智能体强化学习，它是将强化学习的思想和算法应用到多智能体系统中。20世纪90年代，利特曼提出的以马尔可夫决策过程为环境框架的多智能体强化学习[14]，为解决大部分强化学习问题提供了一个简单明确的数学框架。目前，多智能体强化学习系统可以成功应用到多种任务中，包括协作型任务、对抗型任务，以及协作-对抗混合型任务。例如2019年1月，DeepMind公司研制出的人工智能模型AlphaStar在多人战略游戏星际争霸中以较大优势战胜了人类顶级选手，极大地震撼了社会各界。

2.3.2 群智感知

为了解决各种大规模数据需求问题，提供高质量、可靠的数据服务，群智感知逐渐成为群体智能的研究热点之一。2012年，国内最早从事这方面研究的清华大学刘云浩教授提出群智感知的理念是无意识协作，即让用户在不知情的情况下完成感知任务，突破专业人员参与的壁垒[7]。群智感知通过人们已有的移动设备形成交互式的、参与式的感知网络，并将感知任务发布给网络中的个体或群体来完成，从而帮助专业人员或公众收集数据、分析信息和共享知识[15]。与基于传感网和物联网的感知方式不同，群智感知以大量普通用户作为感知源，强调利用大众的广泛分布性、灵活移动性和机会连接性进行感知，并为城市及社会管理提供智能辅助支持。

2.3.3 联邦学习

近些年来，保护用户隐私和防止敏感信息泄露已成为世界性的重大挑战。欧盟于2018年5月25日正式实施《通用数据保护条例》(GDPR)，旨在加强对欧盟境内居民个人数据和隐私的保护。2020年10月13日，十三届全国人大常委会第二十二次会议首次审议了《个人信息保护法(草案)》。2021年6月10日，我国第一部有关数据安全的法律《数据安全法》经十三届全国人大常委会第二十九次会议表决通过，已于2021年9月1日起施行。

在此法律背景下，数据隐私安全已成为群体智能最重要的研究方向之一。如何在保证用户隐私安全的基础上实现数据共享，是群体智能发展的一大难题。谷歌公司在2016年率先提出了基于个人终端设备的“联邦学习”(Federated Learning)算法框架[3]。如图1所示，联邦学习系统中有一个中心服务器和若干客户端，每个客户端利用本地数据对模型进行训练，并将训练好的模型参数上传至服务器，然后服务器聚合并分发参数至客户端。通过这种训练模式，各参与方可以在不披露底层数据和底层数据的加密形态的前提下共建模型。联邦学习由于具有保障隐私的特性，能够降低传统中心化机器学习方法带来的系统性隐私风险和成本。正因为这些优势，联邦学习越来越多地得到学术界和工业界的广泛关注。

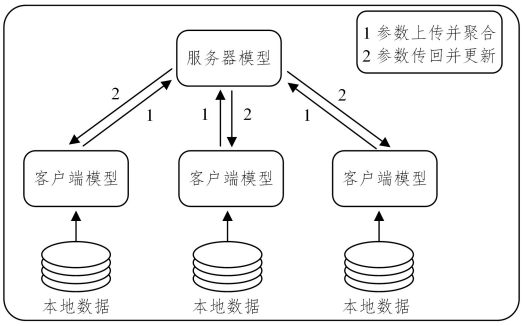

图1 联邦学习框架

Fig. 1 Framework of federated learning

2.4 群体智能的总体趋势

我们可以从这些早期群体智能和部分新兴群智算法中得出，群体智能算法的思想包含两种形式——协作和对抗。从协作的角度来说，所有个体为一个共同的目标服务，个体之间通过协调协作机制达到共同目标。从对抗的角度来说，个体间通过彼此对抗的方式各自优化个体目标，维护个体利益。群体智能中协作和对抗的思想并存，二者相互结合，共同发挥作用，最终达到一种均衡的状态。

3 群体智能中的协作思想

群体智能的概念自提出之时，基本假设就是节点间的协作。本节首先介绍协作在群体智能场景下的含义；其次对几种经典的群体智能算法举例并揭示其中包含的协作思想，包括蚁群优化算法、多智能体系统、群智感知等；接着进一步对联邦学习的协作思想进行详细介绍；最后对这些群体智能的协作算法的共同之处加以总结。

3.1 定义

群体智能中的协作是指个体之间通过协调各自的知识、目的、技巧和规划，从而完成各自的任务或者复杂问题的求解。在群体智能系统中，为了达到共同的目标，个体之间必须进行协作和通信。协作是群体智能的一种协调方式，没有协作，群体智能将会退化为纯粹的个体组合，在共同工作时也达不到预期的目的，甚至会严重影响系统的性能。

3.2 经典群体智能算法中的协作

3.2.1 蚁群算法

蚁群系统(Ant System)[16]是最早的蚁群优化算法，它是一种通过模拟自然界中蚂蚁集体寻径行为的启发式随机搜索算法。我们以求解旅行商问题为例来介绍蚁群系统算法的协作思想。旅行商问题是：给定一个城市的集合以及城市之间的旅行代价，寻找经过每个城市一次且仅一次而最终回到起始城市的最小旅行代价路径。在蚁群系统算法中，每只蚂蚁会以一个特定的概率分布随机选择接下来要访问的城市，进行路径的构造。在t时刻，第k只蚂蚁由城市i转移到城市j的概率$p_{ij}^{k}(t)$由下式决定：

$$p_{ij}^{k}(t)=\begin{cases}\dfrac{[\tau_{ij}(t)]^{\alpha}\cdot[\eta_{ij}]^{\beta}}{\sum\limits_{x\notin c_k}[\tau_{ix}(t)]^{\alpha}\cdot[\eta_{ix}]^{\beta}}, & j\notin c_k\\ 0, & j\in c_k\end{cases} \tag{1}$$

其中，$\tau_{ij}(t)$表示t时刻在城市i，i连线上所有蚂蚁残留的信息素含量；η_{ij}为从城市i转移到城市j的启发函数，具体指两城市间距离的倒数；c_k表示第k只蚂蚁此时的访问城市集合；α和β分别是τ和η在概率计算中所占的比重。在一次迭代后，所有蚂蚁将根据当前自己环游情况对路径上的信息素进行更新。蚁群算法反映了简单个体之间的协作对复杂问题求解的能力。

3.2.2 多智能体系统

在2.3.1小节中，我们提到智能体之间有协作型、对抗型以及协作-对抗混合型3种关系。本小节将介绍智能体之间的关系是完全协作型的多智能体算法。协作意味着多个智能体要共同完成一个目标任务，即此目标的达成与各智能体动作组合得到的联合动作相关。

在大多数情况下，多智能体的联合最优动作是不唯一的，所以智能体之间需要相互协商从而达成最优的联合动作。智能体之间的互相建模可以为多智能体决策提供潜在的协调机制。在联合动作学习(Joint Action Learner，JAL)[17]方法中，智能体会基于观察到的其他智能体的历史动作对其他智能体的策略进行建模。在频率最大Q值(Frequency Maximum Q-value，FMQ)[18]方法中，引入了一种新的个体值函数，该函数考虑了个体动作所在的联合动作取得最优回报的频率，进而在学习过程中引导智能体选择回报最优的联合动作中的自身动作，则所有智能体的最优动作组合被选择的概率也会更高。

上述JAL和FMQ方法的基本思路都是基于均衡求解法，但这类方法通常只能处理小规模的多智能体问题。在大规模多智能体学习问题中，考虑群体联合动作的效应，包括当前智能体受到的影响以及在群体中发挥的作用，对于智能体的策略学习是有较大帮助的。在基于平均场理论的多智能体强化学习(Mean Field MARL，MFMARL)方法[19]中，考虑到集中式全局值函数的学习效果会受到智能体数量的影响，对值函数进行分解。单个智能体j的值函数$Q_j(s,a)$仅需考虑与其相邻的N_j个相邻智能体之间的相互作用：

$$Q_j(s,a)=\frac{1}{N_j}\sum_{k\in N(j)}Q_j(s,a_j,a_k) \tag{2}$$

其中，s 是当前时刻的环境状态，a_j 和 a_k 分别是智能体 j 和智能体 k 采取的动作。

3.2.3 群智感知

群智感知算法主要偏向于实际应用。我们以无人机的应用为例，无人机先对通信环境进行感知，而后根据感知结果进行自主决策。受任务导向、自然地理因素以及无人机执行决策的影响，通信环境会发生动态变化，无人机将重新执行感知任务，以此循环往复，实现灵活智能的无人机无线通信。对整个群体智能协作系统而言，无人机个体的有限智慧通过协作耦合汇聚到一起，构成无人机集群的强大智能。具体而言，在无人机个体有限感知的基础上，群智感知模块采用离散状态获取、全局形势推理、演化趋势预测的思路，实现“由点到面、由当前到未来、由个体智慧汇聚群体智能”的多域立体协同感知。

3.3 联邦学习中的协作

联邦学习算法自提出之时，即被称为一种典型的分布式智能协同协作范例。根据联邦学习的设置，服务器端对会收集到的模型信息进行某种方式的聚合，更新全局模型并分发至客户端。联邦学习可以通过聚合、分发、更新 3 个阶段实现客户端之间的协作

3.3.1 联邦平均算法

联邦平均算法(Federated Average)[3]是最为典型的联邦协作方法。在该方法中，客户端执行本地随机梯度下降，服务器端执行模型平均。首先，随机选择一定数量的客户端，使用本地数据集在本地运行若干次随机梯度下降训练模型；然后，这些客户端将更新的模型参数或梯度发送至服务器端；随后，服务器端对更新的本地模型进行平均，形成更新的全局模型。联邦平均算法的总损失函数 $f(w)$ 是各个客户端本地损失的加权平均：

$$\begin{cases}f(w)=\sum_{k=1}^{K}\frac{n_k}{n}F_k(w)\\F_k(w)=\frac{1}{n_k}\sum_{i\in P_k}f_i(w)\end{cases} \tag{3}$$

其中，K 为客户端数量，P_k 表示客户端 k 的本地数据集，$n_k=|P_k|$ 为数据规模，$f_i(w)=l(x_i,y_i;w)$ 表示客户端在第 i 个样本 (x_i,y_i) 以及模型参数 w 下的预测损失。根据各个客户端的本地损失计算得到全局损失后，服务器端的全局更新公式为：

$$w_{t+1}\leftarrow w_t-\eta\nabla f(w_t) \tag{4}$$

其中，w_t 和 w_{t+1} 分别是第 t 轮和第 $t+1$ 轮迭代过程的全局模型参数，η 是学习率。客户端和服务器端通过参数互传的方式在分布式设置下进行多方协作训练模型，传递模型知识。

3.3.2 联邦蒸馏算法

联邦平均算法是通过平均模型参数或梯度进行客户端间信息的传递。然而，针对联邦学习中的模型异构问题(即客户端模型架构和大小不相同)，这种方法便不再适用。为了解决这种问题，异构模型融合方法(FedDF)[20]将集成蒸馏技术[21]运用在联邦学习的模型聚合中。

异构模型融合方法分为两个阶段：第一阶段与联邦平均算法相同，客户端需要将更新的模型参数发送至服务器端；第二阶段中，服务器端加权平均来自客户端的模型参数后，再通过未标记的数据或通过生成器生成的数据进行集成蒸馏，得到更新的模型参数。集成蒸馏是指将客户端老师模型蒸馏到一个服务端学生模型，通过集成蒸馏，每种模型架构都能够从模型平均输出中获取知识，从而实现模型结构不同的客户端间的协作。

3.4 协作思想总结

如上所述，群体智能中不同研究领域(蚁群算法、协作型多智能体系统、群智感知、联邦学习等)通过不同的协作机制来达到群体智能系统的共同优化目标。这些协作机制都是通过将个体间的知识进行某种程度的聚合、集成以及推理，把个体的有限智慧耦合汇聚成群体的强大智能。而联邦学习相较于其他群智算法的优点在于：联邦学习在个体协作的过程中同时保持个体的隐私并且保证了个体的各异性，因而更适合现实场景的群体协作。

4 群体智能中的对抗思想

群体智能中仅仅只有协作是不够的，协作本身是具有一定的局限性的，可能会导致个体间过分依赖，也可能会导致系统的不公平性。例如联邦平均算法中服务器每次只能选择一定批量的客户端参与训练，这可能会导致计算能力较强的客户端被选择的概率较大，较差的客户端被选择的概率较小。这种局限性可以通过个体之间的对抗克服。在本节中，我们首先介绍群体智能中对抗的含义，并对典型的对抗性质的群体智能算法进行介绍，包括狼群算法、多智能体强化学习系统以及联邦学习和群智感知中的激励机制。最后，讨论了对抗思想应用到联邦学习的研究前景和挑战。

4.1 定义

根据对抗思想不同，我们将群体智能的对抗分为数据拟合角度下的对抗和博弈角度下的对抗。数据拟合角度下的对抗是指通过搜索策略或者超参数优化等算法对数据进行拟合，对模型进行优化，最终能够得到最优解，即使得目标函数值效果最好，模型的平均损失达到最小的解。博弈角度下的对抗是指理性决策者之间存在利益冲突时如何为自身谋取最大利益。博弈的最终目标是达到纳什均衡(Nash Equilibrium，NE)[22]，即在其他决策者策略不变的情况下，任何一个决策者改变当下的决策，都无法得到更多的收益。最经典的例子就是囚徒困境(Prisoner's Dilemma)。：两名嫌犯都有认罪和沉默两种行为可以选择，对二人来说，最优解应当是两人同时保持沉默，导致警方仅能依靠已有的犯罪事实对两人轻判，但是对于两个嫌犯来说，认罪才是对自己最有利的行动，最终的结果就是两人同时认罪而得到应有的惩罚。博弈思想在经典群体智能算法中的应用非常广泛。

4.2 经典群体智能算法中的对抗

4.2.1 狼群算法

狼群算法[12]是一种数据拟合角度下的对抗算法。它是基于狼群的群体智能，模拟狼群捕食行为及其猎物分配方式提出的一种群体智能算法。狼群算法中提出了：1)“胜者为王”的头狼产生规则，即在迭代过程中，将每次迭代后最优狼的目标函数值与前一代中头狼的值进行比较，若更优则对头狼位置进行更新；2)“强者生存”的狼群更新机制，即猎物按照“由强到弱”的原则进行分配，导致弱小的狼会被饿死，亦即在算法中去除目标函数值最差的若干匹人工狼，同时随机产生同等数量的人工狼。这种头狼产生规则和狼群更新机制，促使

狼群向最有可能再次捕获到猎物的方向繁衍发展，同时也体现了对抗思想在群体智能中是不可或缺的。

4.2.2 多智能体系统

博弈论在多智能体强化学习中有着广泛的应用。在智能体之间是完全对抗关系的随机博弈中，智能体的回报函数是相反的，环境通常存在两个完全敌对的智能体，智能体的目标是最大化自身的回报，同时尽可能最小化对方回报。最有代表性的算法是 Min-Max Q-learning 算法[14]，该算法可以用于两个智能体之间是完全对抗关系的零和随机博弈情形，其使用最小最大化的思想求解每个特定状态的阶段博弈的纳什均衡策略。式(5)为智能体的最优回报函数，其含义为智能体需要考虑在其他智能体采取的动作令自己回报最差的情况下，能够获得的最大期望回报。这种方式使得智能体容易收敛到纳什均衡策略。

$$V^*(s)=\max_{\pi}\min_{a^-}\sum_{a}Q^*(s,a,a^-)\pi(s,a) \tag{5}$$

其中，a^- 表示智能体 a 的对手，s 和 π 分别指当前环境状态和智能体 a 的策略，$V^*(s)$ 为第 i 个智能体的状态值函数，$Q^*(s,a,a^-)$ 为联结动作状态值函数。

此外，典型的完全对抗型算法还有纳什 Q-Learning 算法[23]，该算法在 Min-Max Q 算法的基础上进一步将适用范围扩展到多人一般和博弈。这种算法最常见的应用有集群对抗，大到战场对抗，小到各类比赛的战术战略，集群对抗均是未来战场的重要作战模式。

4.2.3 群智感知激励机制

基于博弈论的对抗思想还有利于实现群体智能中资源的有效配置。为了提高参与方的积极性，如何评估各个参与方的贡献量并给予一定的奖励，对于群智感知系统来说是一大重要议题。在群智感知激励方式中，报酬支付激励方式主要是基于博弈论的方法，其中最主要的是拍卖机制。拍卖机制能够提供很好的数学模型来解决理性服务器和参与者之间的冲突和合作的关系以及决定选择问题。在拍卖机制中，服务器平台和参与者被视作博弈的双方，同时参与者之间为获得感知任务形成对抗关系。根据拍卖双方的人数、信息是否完全、优化目标等的不同，不同的拍卖方式适用于不同的群智感知环境。报酬支付能够有效激励参与者的积极性[24]。

4.3 联邦学习的对抗

由于联邦学习是一种基于模型共享的群体智能算法，所以目前大多数学者依然是在协作的基础上对其进行改进。对抗思想较少被应用到联邦学习中。在联邦场景中，参与者之间设备通信能力不同或者数据分布以及模型存在差异，使得各个参与者的优化目标有所不同，而博弈对抗的思想恰恰更适用于优化目标不同的场景。因此本文认为，对抗思想在联邦学习中的应用具有非常大的科研价值和挑战性。

当前博弈对抗的思想在联邦学习中的应用仅仅停留在激励机制的设计上[25]，与上述群智感知的激励机制相似。我们认为这种思想可以更进一步地在联邦学习优化算法中发挥作用。

4.3.1 生成对抗网络在联邦学习中的应用

生成对抗网络(Generative Adversarial Network，GAN)是一个强大的基于博弈论的生成模型学习框架。该模型由 GoodFellow 在 2014 年首次提出[26]。其基本思想源自二人零和博弈，由一个生成器和一个判别器构成，通过对抗学习的方式来迭代训练，逼近纳什均衡。近两年涌现出越来越多关于生成对抗网络和联邦学习结合的工作。我们可以根据其出发点的不同将这些工作分为 3 类。

(1)数据检测和数据质量的提升。联邦扩充方(Federated Augmentation，FAug)[27]可以扩充本地数据集以生产独立同分布数据。具体做法是在服务器端根据种子数据样本训练一个生成性对抗网络，每个设备下载生成器来补充其目标标签。谷歌团队针对联邦学习场景下数据无法进行人工检查的问题，也提出用联邦学习场景下训练的 GAN 来对常见的数据问题进行检查[28]。

(2)攻击和防御问题。这类工作主要考虑了联邦场景中受到的 GAN 攻击以及如何用 GAN 进行防御。由于联邦学习中服务器端无法获取各客户端的数据，所以可以在服务器设置一个 GAN 来产生一个测试数据集，利用各客户端本地模型在此数据集上的打分来判断哪个客户端是攻击者[29-30]。

(3)分布式 GAN 的优化。这类工作主要解决分布式 GAN 中存在的数据单一性和参数更新等问题。一种较为直觉的办法是每个客户端设置一个 GAN 在本地进行更新后，再将参数或梯度传递至服务器进行加权平均[31-32]。此外，有学者使用临时鉴别器训练分布式 GAN 的方法，此方法通过学习一个有多个数据中心的本地鉴别器组成的自适应生成器，很好地解决了如何用临时鉴别器更新生成器的参数问题[33]。

我们可以从上述工作中得到启发并进一步展望这一领域的研究方向。上述方法一方面是在特定任务上将 GAN 作为一种附加技术辅助联邦学习(前两类工作)，另一方面是在分布式 GAN 的基础上加入联邦学习的模式进行训练(第三类工作)。我们重点关注第三类工作，在这类工作中，可以在服务器端设置单个鉴别器，在客户端设置多个生成器(见图 2 左)；或者在服务器端设置单个生成器，在服务器端设置多个鉴别器(见图 2 右)。如此一来，单个生成器和若干个鉴别器(或者单个鉴别器和若干生成器)之间的博弈过程即为服务器和客户端之间的博弈，最终可以使得联邦系统达到纳什均衡。

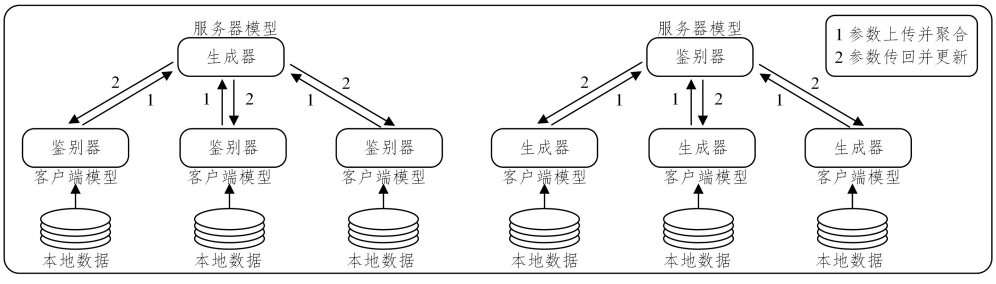

图 2 生成对抗网络在联邦学习中的两种应用设置

Fig. 2 Twosettings of generative adversarial networks in federated learning

4.3.2 强化学习在联邦学习中的应用

除了生成对抗网络外，强化学习(尤其是多智能体强化学习)也是非常值得关注的。如何将强化学习的思想应用到联邦学习中，目前也是一个非常值得研究的开放性问题。

(1)单智能体强化学习的应用。在联邦学习的训练过程中，每回合均需要从海量客户端中选择出一定数目的客户端，即在每个回合均需做出决策并执行动作。强化学习可以解决这种决策问题，于是有学者使用了强化学习经典算法 Deep Q-learning 训练智能体学习如何选择每轮参与训练的客户端，以最大化一个鼓励提升正确率并处罚使用更多通信次数的奖励[34]。其中，状态是客户端的本地模型权重和服务器的全局模型权重；动作是指对客户端进行选择，选择不同设备对应的 Q 值也是不同的 Q 值。奖励是测试精度，从而激励智能体选择设备达到更高的测试精度。

(2)多智能强化学习的应用。从系统架构的角度来说，多智能体系统和联邦学习是非常相似的。联邦学习中的客户端可以看作是多个智能体。我们可以考虑借鉴对抗型多智能体强化学习中的对抗思想(例如极大极小化思想)，在联邦学习系统中引入竞争机制，客户端可以将其他客户端看作分布式对手，则每个客户端的优化目标变为在其余客户端最小化自身精度的情况下最大化自身精度，在彼此竞争的情况下使得系统达到均衡状态。

4.4 对抗思想总结

从上述群体智能算法中我们可以看出，群体智能中的对抗能够提高模型效率并促进系统的公平。狼群算法、对抗型多智能体强化学习和群智感知等算法分别体现了数据拟合角度和博弈角度的对抗思想。对抗思想在联邦学习中的应用目前尚处于初步探索阶段，仍有许多开放性问题值得研究。本文将生成对抗网络和强化学习在联邦学习中的应用进行了总结并提出了新的研究方向。同时，我们也坚定地相信，这一方向具有非常重要的研究价值和广阔的研究前景。

5 协作对抗并存的分布式群智

协作性是群体智能的宏观特征。群体智能在早期被提出的时候，其前提便是以群体之间的协作为基础——从模拟蚂蚁间传递信息素的蚁群优化算法，到模拟鸟类协作捕食的粒子群算法，到协同通信的群智感知和多智能体系统，再到节点间共享模型参数的联邦学习，皆是如此。

对抗性是群体智能的必要形式。群体智能中的对抗是指在个体或小范围群体间目标不完全一致、优化方向冲突时，单个个体性能的提升可能会导致其他个体性能的下降，此时则需要个体间彼此通过某种对抗机制来达到自己的利益，并同时保证群体也得到一定程度的优化。

综上所述，群体智能算法中，协作与对抗有着共同的本质特征，均是实现个体目标和群体目标的手段，根本目的都是达到利益最大化，具体取决于个体目标和总体目标是否一致。协作与对抗互为包容，浑然一体，可以用适当的形式把它们统一起来。这就需要找出对抗与协作的内在联系并将它们一体化。

进一步来讲，我们可以扩大当前讨论的领域范围，放眼到社会群体中。企业间的主流思想是对抗性协作，即通过协作修正对抗过程中的弊端，实现非零和博弈，在这一过程中，协作只是提升对抗能力的一种方式与手段，最终逐渐形成一种对抗与协作并存的对抗性战略。同样的道理在群体智能中也是适用的，协作与对抗共同发挥作用，从而使得系统达到均衡状态。协作机制与对抗机制并存。在对抗的基础上实现协作，协作的局面中存在对抗，以对抗促协作，协作中存对抗，是群体智能的精髓所在。

6 群体智能生态

无论是基于协作还是对抗，构建群体智能生态，不仅需要前述群智算法的研究，还需要制定系统的运行规则，或者构建一个支持群体智能的生态环境，此生态环境为协作与对抗并存的群体智能提供信任基础、经济模型和争端解决机制。具体而言，这样一个群体智能的生态系统应该包含以下 4 个方面的规则。

(1)可信机制。可信是协作的基础，甚至一定程度上也为公平的博弈提供基础。因此群体智能中所利用的数据、训练的模型，以及建模和运算过程，需要一种可信机制来验证数据的真实性和质量、建模过程合规性、结果可溯源性等。目前在可信计算和可信建模上的研究很多，未来有望为群体智慧提供可信基础机制；同时，区块链也为分布式环境提供了一种可信的基础设施和协议，未来将研究如何基于智能合约实现对数据和建模过程的真实可信记录。

(2)激励和流通机制。群体智能生产要素(数据、模型、算力等)往往是分离的，因此需要激励和流通机制推动要素有效配置。同时，当多个节点进行协同时，也会出现合作博弈中的绩效分配问题(Credit Assignment)，为了在模型层面实现收益分配，需要准确衡量数据的价值。近年来有众多研究开始关注数据定价问题，这其中的定价方法、节点贡献度评价方法等可以被看作群体智慧的激励机制。

(3)争端解决机制。群体智能存在对抗，当节点目标不一致时，可采用前述的博弈对抗方式取得系统均衡。然而，由于目标差异太大，均衡状态可能与系统目标有很大差距，造成整个群体智能的低效，因此需要一种机制解决争端，避免系统陷入低效陷阱。在这方面，区块链上的共识机制已经有了一些相关研究，未来可以考虑如何将其应用到分布式建模环境下，以解决争端。

(4)治理机制。为了实现分布式群智生态系统的整体目标，需要引入将系统整体目标转化为个体和交互规则的治理机制，可以考虑利用反向博弈论等方法，根据整个群体智慧的系统目标来推演出适用于个体的智能合约。

结束语 本文首先介绍了群体智能算法的协作和对抗方法，对经典群体智能算法进行阐述。未来的研究方向是在联邦学习生态中引入博弈对抗的思想，使得系统达到均衡状态。本文认为，协作和对抗缺一不可，以对抗促协作，协作中存对抗，构建协作与对抗并存的群体智能生态，是群体智能的必然发展趋势。

参 考 文 献

[1] BENI G. The concept of cellular robotic system [C]// Proceedings IEEE International Symposium on Intelligent Control

1988. IEEE，1988：57-62

[2] ZHAO J，ZHANG X T，LI J M，et al. Research review of crowd intelligence 2.0 [J]. Computer Engineering，2019，45(12)：7.

[3] MCMAHAN B，MOORE E，RAMAGE D，et al. Communication-efficient learning of deep networks from decentralized data [C]// Artificial Intelligence and Statistics. PMLR，2017：1273-1282.

[4] DORIGO M，GAMBARDELLA L M. Ant colonies for the traveling salesman problem[J]. Biosystems，1997，43(2)：73-81.

[5] KENNEDY J，EBERHART R. Particle swarm optimization [C]// ICNN95-International Conference on Neural Networks. 2002.

[6] LIU J，CHEN Z Q，LIU Z X. Research Progress of Multi-agent System and its Cooperative Control [J]. Journal of Intelligent Systems，2010，5(1)：1-9.

[7] LIU Y H. Crowd Sourcing computing[J]. Communications of the China Computer Federation，2012，8(10)：38-41.

[8] SUN J，WANG J，CHEN J，et al. Cooperative communication based on swarm intelligence：vision，model，and key technology [J]. SCIENTIASINICA Informationis，2020，50(3)：307-317.

[9] DUAN H，QIU H. Unmanned aerial vehicle swarm autonomous control based on swarm intelligence[M]. Beijing：Science Press，2018.

[10] LAN S F，LIU S. Overview of research on Cuckoo search algorithm[J]. Computer Engineering and Design，2015，36(4)：1063-1067.

[11] LI X L. A New Intelligent Optimization Method-Artificial Fish School Algorithm [D]. Hangzhou：Zhejiang University，2003.

[12] WU H，ZHANG F，WU L. New swarm intelligence algorithm—wolf pack algorithm [J]. System Engineering and Electronics，2010，35(11)：2430-2438.

[13] ZHANG W，MEI H. A constructive model for collective intelligence[J]. National Science Review，2020，7(8)：1273-1277.

[14] LITTMAN M L. Markov games as a framework for multi-agent reinforcement learning [C] // Machine Learning Proceedings 1994. Elsevier，1994：157-163.

[15] WU Y，ZENG J R，PENG H，et al. Survey on incentive mechanisms for crowd sensing[J]. Ruan Jian Xue Bao/Journal of Softwar，2016，27(8)：2025-2047.

[16] DORIGO M，MANIEZZO V，COLORNI A. Ant system：optimization by a colony of cooperating agents[J]. IEEE Transactions on Systems，Man，and Cybernetics，Part B(Cybernetics)，1996，26(1)：29-41.

[17] CLAUS C，BOUTILIER C. The dynamics of reinforcement learning in cooperative multi-agent systems[C]// Proc. AAAI-98. 1998.

[18] SPIROS K，DANIEL K. Reinforcement learning of coordination in cooperative mas[C]// The 18th National Conference on AI. Alberta，Canada：ACM Press. 2002：326-331.

[19] YANG Y，LUO R，LI M，et al. Mean field multi-agent reinforcement learning[C]// International Conference on Machine Learning. PMLR，2018：5571-5580.

[20] LIN T，KONG L，STICH S U，et al. Ensemble distillation for robust model fusion in federated learning [J]. arXiv：2006.07242，2020.

[21] HINTON G，VINYALS O，DEAN J. Distilling the knowledge in a neural network[J]. arXiv：1503.02531，2015.

[22] NASH J F. Equilibrium points in n-person games[J]. Proceedings of the National Academy of Sciences，1950，36(1)：48-49.

[23] HU J，WELLMAN M P. Nash q-learning for general-sum stochastic games[J]. Journal of Machine Learning Research，2003，4(Nov)：1039-1069.

[24] WU Y，ZENG J R，PENG H，et al. Survey on incentive mechanisms for crowd sensing[J]. Journal of Software，2016，27(8)：2025-2047.

[25] NG K L，CHEN Z，LIU Z，et al. A multi-player game for studying federated learning incentive schemes[C]// Proceedings of the 29th International Joint Conference on Artificial Intelligence (IJCAI 2020). 2020：5179-5281.

[26] GOODFELLOW I J，POUGET-ABADIE J，MIRZA M，et al. Generative adversarial networks[J]. arXiv：1406.2661，2014.

[27] JEONG E，OH S，KIM H，et al. Communication-efficient on-device machine learning：Federated distillation and augmentation under non-iid private data[J]. arXiv：1811.11479，2018.

[28] AUGENSTEIN S，MCMAHAN H B，RAMAGE D，et al. Generative models for effective ml on private，decentralized datasets[J]. arXiv：1911.06679，2019.

[29] ZHANG J，CHEN J，WU D，et al. Poisoning attack in federated learning using generative adversarial nets[C]// 2019 18th IEEE International Conference on Trust，Security and Privacy in Computing And Communications/13th IEEE International Conference On Big Data Science and Engineering (TrustCom/BigDataSE). IEEE，2019：374-380.

[30] ZHAO Y，CHEN J，ZHANG J，et al. Pdgan：a novel poisoning defense method in federated learning using generative adversarial network[C]// International Conference on Algorithms and Architectures for Parallel Processing. Springer，2019：595-609.

[31] RASOULI M，SUN T，RAJAGOPAL R. Fedgan：Federated generative adversarial networks for distributed data [J]. arXiv：2006.07228，2020.

[32] FAN C，LIU P. Federated generative adversarial learning[C]// Chinese Conference on Pattern Recognition and Computer Vision(PRCV). Springer，2020：3-15.

[33] QU H，ZHANG Y，CHANG Q，et al. Learn distributedgan with temporary discriminators[C]// European Conference on Computer Vision. Springer，2020：175-192.

[34] WANG H，KAPLAN Z，NIU D，et al. Optimizing federated learning on non-iid data with reinforcement learning[C]// IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE，2020：1698-1707.

ZHU Di-di，born in 1998，postgraduate. Her main research interests include federated learning and domain adaptation.

WU Chao，born in 1972，Ph.D，professor，Ph.D supervisor. His main research interests include federated learning and so on.